SS2R24G4i, SS2R48G4i

Layer 2/Layer4 Managed Fast Ethernet Switch

USER MANUAL

Version 1.2

March 2009

Trademarks

Copyright ©2009 Amer.com.
Contents subject to change without prior notice.

Copyright Statement

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission, as stipulated by the United States Copyright Act of 1976.

Technical Support Contact

www.amer.com/support

support@amer.com

info@amer.com

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

EMC

EN55022(1988)/CISPR-22(1985)	class A
EN60555-2(1995)	class A
EN60555-3	
IEC1000-4-2(1995)	4K V CD, 8KV, AD
IEC1000-4-3(1995)	3V/m
IEC1000-4-4(1995)	1KV – (power line), 0.5KV – (signal line)

Preface

SS2R24/48G4i switch is a high performance Ethernet switch which has wire-speed Layer 2 switching capacity.

The switch can seamlessly support various network interfaces from 10Mb, 100Mb, 1000Mb Ethernets.

We strongly recommend you to read through this manual carefully before installation and configuration to avoid possible damage to the switch and malfunction.

CONTENTS

Chapter 1 Switch Overview ____ **1**

1.1 BRIEF INTRODUCTION ____ 1
1.1.1 Overview ____ 1
1.1.2 Features and Benefits ____ 2
1.1.3 Main Features ____ 3

1.2 TECHNICAL SPECIFICATIONS ____ 4

1.3 PHYSICAL SPECIFICATIONS ____ 5

1.4 PRODUCT APPEARANCE ____ 5
1.4.1 Product Front Panel View ____ 5
1.4.2 Product back panel view ____ 5
1.4.3 Status LEDs ____ 6

Chapter 2 Hardware Installation ____ **8**

2.1 INSTALLATION NOTICE ____ 8
2.1.1 Environmental Requirements ____ 8
2.1.2 Installation Notice ____ 10
2.1.3 Security Warnings ____ 11

2.2 INSTALLATION PREPARATION ____ 11
2.2.1 Verify the Packet Contents ____ 11
2.2.2 Required Tools and Utilities ____ 11

2.3 HARDWARE INSTALLATION ____ 12
2.3.1 Installing the Switch ____ 12
2.3.2 Connecting Console ____ 12
2.3.3 Power Supply Connection ____ 13

Chapter 3 Setup Configuration ____ **15**

3.1 SETUP CONFIGURATION ____ 15

3.2 MAIN SETUP MENU ____ 15

3.3 SETUP SUBMENU ____ 15
3.3.1 Configuring switch hostname ____ 15
3.3.2 Configuring Vlan1 Interface ____ 16
3.3.3 Telnet Server Configuration ____ 16
3.3.4 Configuring Web Server ____ 17
3.3.5 Configuring SNMP ____ 17
3.3.6 Exiting Setup Configuration Mode ____ 18

Chapter 4 Switch Management ____ **20**

4.1 MANAGEMENT OPTIONS ____ 20

4.1.1 Out-of-band Management 20
4.1.2 In-band Management 23

4.2 MANAGEMENT INTERFACE 26
4.2.1 CLI Interface 27
4.2.2 Web Interfac 32

Chapter 5 Basic Switch Configuration 34

5.1 BASIC SWITCH CONFIGURATION COMMANDS 34
5.1.1 clock set 34
5.1.2 config 34
5.1.3 exit 34
5.1.4 help 35
5.1.5 ip host 35
5.1.6 ip http server 35
5.1.7 hostname 35
5.1.8 reload 35
5.1.9 setup 36
5.1.10 language 36
5.1.11 web-user 36
5.1.12 write 36
5.1.13 show cpu usage 37

5.2 MONITOR AND DEBUG COMMAND 37
5.2.1 Ping 37
5.2.2 Telnet 37
5.2.3 SSH 40
5.2.4 Traceroute 44
5.2.5 Show 44
5.2.6 Debug 46

5.3 CONFIGURE THE IP ADDRESS OF THE SWITCH 46

5.4 SNMP CONFIGURATION 48
5.4.1 Introduction To SNMP 48
5.4.2 Introduction to MIB 49
5.4.3 Introduction to RMON 50
5.4.4 SNMP Configuration 50
5.4.5 Typical SNMP Configuration Examples 52
5.4.6 SNMP Troubleshooting 53

5.5 SWITCH UPGRADE 56
5.5.1 BootROM Upgrade 57
5.5.2 FTP/TFTP Upgrade 58

5.6 THE THREE-LEVEL SWITCH OF LOG MESSAGE 61
5.6.1 Introduction to the system log 61
5.6.2 Configuring The System Log 63

5.6.3 System Log Configuration Example ____ 64
5.6.4 System Log troubleshooting ____ 64

5.7 CLASSIFIED CONFIGURATION ____ 66
5.7.1 Introduction of Classified Configuration ____ 66
5.7.2 Configure the Classified Configuration ____ 66

5.8 PORT ISOLATION ____ 66
5.8.1 Introduction of Port Isolation ____ 66
5.8.2 Port Isolation Configuration ____ 67

Chapter 6 Cluster Configuration ____ 68

6.1 INTRODUCTION TO CLUSTER NETWORK MANAGEMENT ____ 68

6.2 CLUSTER NETWORK MANAGEMENT CONFIGURATION ____ 68
6.2.1 Cluster Network Management Configuration Sequence ____ 68

Chapter 7 Port Configuration ____ 71

7.1 PORT INTRODUCTION ____ 71

7.2 PORT CONFIGURATION ____ 71
7.2.1 Port Configuration ____ 71
7.2.2 VLAN Interface Configuration ____ 73
7.2.3 Port Mirroring Configuration ____ 73

7.3 PORT CONFIGURATION EXAMPLE ____ 76

7.4 PORT TROUBLESHOOTING ____ 77
7.4.1 Monitor and Debug Command ____ 77

Chapter 8 MAC Table Configuration ____ 78

8.1 INTRODUCTION TO MAC TABLE ____ 78
8.1.1 Obtaining MAC Table ____ 78
8.1.2 Forward or Filte ____ 79

8.2 COMMANDS FOR MAC ADDRESS TABLE CONFIGURATION ____ 80
8.2.1 mac-address-table aging-time ____ 80
8.2.2 mac-address-table ____ 80
8.2.3 mac-address-table blackhole ____ 80
8.2.4 clear mac-address-table dynamic ____ 81

8.3 TYPICAL CONFIGURATION EXAMPLE ____ 81

8.4 TROUBLESHOOTING ____ 81
8.4.1 Monitor and Debug Command ____ 81
8.4.2 Troubleshooting ____ 82

8.5 MAC ADDRESS FUNCTION EXTENSION ____ 82
8.5.1 MAC Address Binding ____ 82

Chapter 9 VLAN Configuration ____ 86

9.1 INTRODUCTION TO VLAN ____ 86
9.2 VLAN CONFIGURATION ____ 87
9.2.1 VLAN Configuration Task List ____ 87
9.2.2 Typical VLAN Application ____ 89
9.3 DOT1Q-TUNNEL CONFIGURATION ____ 90
9.3.1 Dot1q-tunnel Introduction ____ 90
9.3.2 Configuration Task Sequence Of Dot1q-Tunnel ____ 91
9.3.3 Typical Applications Of The Dot1q-tunnel ____ 92
9.3.4 Dot1q-tunnel Troubleshooting ____ 93
9.4 PROTOCOL VLAN CONFIGURATION ____ 93
9.4.1 Protocol VLAN Introduction ____ 93
9.4.2 Protocol VLAN Configuration Task Sequence ____ 94
9.4.3 Protocol VLAN Troubleshooting ____ 94
9.5 VLAN TROUBLESHOOTING ____ 94
9.5.1 Monitor and Debug Comman ____ 94
Chapter 10 RSTP CONFIGURATION ____ 96
10.1 INTRODUCTION TO RSTP ____ 96
10.2 RSTP CONFIGURATION ____ 97
10.2.1 RSTP CONFIGURATION TASK SEQUENCE ____ 97
10.3 RSTP CONFIGURATION EXAMPLES ____ 98
10.4 RSTP TROUBLESHOOTING ____ 100
10.4.1 Monitor and Debug Command ____ 100
10.4.2 RSTP TROUBLESHOOTING ____ 101
Chapter 11 IGMP Snooping ____ 102
11.1 INTRODUCTION TO IGMP SNOOPING ____ 102
11.2 IGMP SNOOPING CONFIGURATION ____ 102
11.2.1 IGMP Snooping Configuration Task ____ 102
11.3 IGMP SNOOPING EXAMPLES ____ 104
11.4 IGMP SNOOPINGIGMP SNOOPING TROUBLESHOOTING ____ 106
11.4.1 IGMP Snooping Monitor and Debug Command ____ 106
11.4.2 IGMP Snooping Troubleshooting ____ 107
Chapter 12 Multicast VLAN Configuration ____ 108
12.1 MULTICAST VLAN INTRODUCTION ____ 108
12.2 MULTICAST VLAN CONFIGURATION ____ 108
12.2.1 Multicast VLAN Configuration Task Sequence ____ 108
12.3 MULTICAST VLAN EXAMPLES ____ 109
Chapter 13 DCSCM Configuraion ____ 111

13.1 DCSCM INTRODUCTION ____ 111
13.2 DCSCM CONFIGURATION ____ 111
13.2.1 DCSCM Configuration Task Sequence ____ 111
13.3 DCSCM TYPICAL EXAMPLES ____ 114
13.4 DCSCM TROUBLESHOOTING ____ 115
13.4.1 DCSCM Debug and Monitor Command ____ 115
13.4.2 11.4.2 DCSCM Troubleshooting ____ 116
Chapter 14 802.1x Configuration ____ 117
14.1 INTRODUCTION TO 802.1X ____ 117
14.2 802.1X CONFIGURATION ____ 118
14.2.1 802.1x Configuration Task List ____ 118
14.3 EXAMPLE OF 802.1X APPLICATION ____ 122
14.4 802.1X TROUBLESHOOTING ____ 123
14.4.1 802.1x Monitor and debug command ____ 123
14.4.2 802.1x Troubleshooting ____ 127
Chapter 15 ACL Configuration ____ 128
15.1 INTRODUCTION TO ACL ____ 128
15.2 ACCESS-LIST ____ 128
15.2.1 Access-group ____ 128
15.2.2 Access-list Action and Global Default Action ____ 128
15.3 ACL CONFIGURATION ____ 129
15.3.1 ACL Configuration Task Sequence ____ 129
15.4 ACL EXAMPLE ____ 139
15.5 ACL TROUBLESHOOTING ____ 142
15.5.1 Monitor And Debug Command ____ 142
15.5.2 ACL Troubleshooting ____ 143
Chapter 16 AM Configuration ____ 145
16.1 AM INTRODUCTION ____ 145
16.2 AM POOL ____ 145
16.3 AM CONFIGURATION ____ 145
16.3.1 AM Configuration Task Sequence ____ 145
16.4 AM EXAMPLES ____ 146
16.5 AM TROUBLESHOOTING ____ 147
16.5.1 AM Debug and Monitor Command ____ 147
16.5.2 AM Troubleshooting ____ 148
Chapter 17 Port Channel Configuration ____ 149

17.1 INTRODUCTION TO PORT CHANNEL ____ 149
17.2 PORT CHANNEL CONFIGURATION ____ 150
17.2.1 Port Channel Debug and Monitor Command ____ 150
17.3 PORT CHANNEL EXAMPLE ____ 151
17.4 PORT CHANNEL TROUBLESHOOTING ____ 153
17.4.1 Debug and Monitor Command ____ 153
17.4.2 Port Channel Channel Troubleshooting ____ 155
Chapter 18 DHCP Configuration ____ 156
18.1 INTRODUCTION TO DHCP ____ 156
18.2 DHCP SERVER CONFIGURATION ____ 157
18.2.1 DHCP Sever Configuration Task List ____ 157
18.2.2 DHCP Server Configuration Commands Example ____ 159
18.3 DHCP TROUBLESHOOTING ____ 160
18.3.1 Monitor and Debug Commands ____ 160
18.3.2 DHCP Troubleshooting ____ 163
Chapter 19 DHCP snooping Configuration ____ 164
19.1 DHCP SNOOPING INTRODUCTION ____ 164
19.2 DHCP SNOOPING CONFIGURATION ____ 164
19.2.1 DHCP Snooping Configuration Task Sequenc ____ 164
19.2.2 DHCP Snooping Typical Applications ____ 166
19.3 DHCP SNOOPING TROUBLESHOOTING ____ 167
19.3.1 Monitor and Debug Information ____ 167
19.3.2 DHCP SnoopingTroubleshooting ____ 168
Chapter 20 Defense Against Segment Scanning ____ 169
20.1 DEFENSE AGAINST SEGMENT SCANNING ____ 169
20.1.1 Defense Against Segment Scanning Configuration Task Sequence 169
20.1.2 Monitor and Debug Command ____ 170
Chapter 21 SNTP Configuration ____ 171
21.1 COMMANDS FOR SNTP ____ 171
21.1.1 sntp server ____ 171
21.1.2 sntp polltime ____ 171
21.1.3 sntp timezone ____ 171
21.1.4 show sntp ____ 172
21.1.5 debug sntp ____ 172
21.2 TYPICAL SNTP CONFIGURATION EXAMPLES ____ 173
Chapter 22 QoS Configuration ____ 174
22.1 INTRODUCTION TO QOS ____ 174

22.1.1 QoS Terms _____ 174
22.1.2 QoS Implementation _____ 175
22.1.3 Basic QoS Model _____ 175
22.2 QOS CONFIGURATION _____ 176
22.2.1 QoS Configuration Task List _____ 176
22.3 QOS EXAMPLE _____ 179
22.4 QOS TROUBLESHOOTING _____ 181
22.4.1 QoS Monitor And Debug Command _____ 181
22.4.2 Qos Troubleshooting _____ 184
Chapter 23 Layer 3 Configuration _____ 185
23.1 LAYER3 INTERFACE _____ 185
23.1.1 Introduction to Layer3 Interface _____ 185
23.1.2 Layer3 interface configuration _____ 185
23.2 ARP _____ 186
23.2.1 Introduction to ARP _____ 186
23.2.2 ARP Forwarding Troubleshooting _____ 186

Chapter 1 Switch Overview

1.1 Brief Introduction

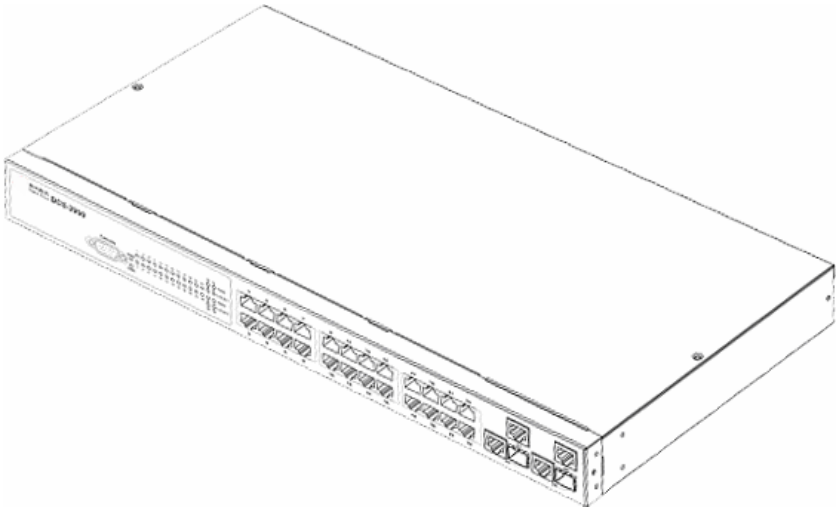


Fig 1-1 SS2R24G4i switch

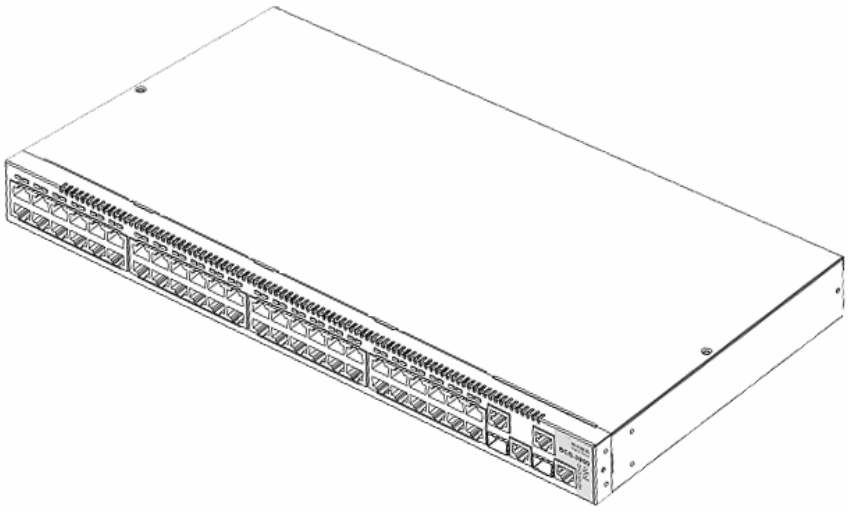


Fig 1-2 SS2R48G4i switch

1.1.1 Overview

The SS2R24/48G4i switch Intelligent Stackable Secure Ethernet Access Switch can not only be utilized in large-scale enterprise networks，campus networks and metropolitan area networks as access equipment, but also can meet the demand for network of medium-scale office environment. This series

of switch has unique network access functions and flexible management of network, including MAC binding/filtering, limiting the total number of Mac addresses, IEEE802.1Q VLAN, PVLAN, IEEE802.1x access authentication, QoS, ACL, bandwidth control, IEEE802.3ad TRUNK, IGMP Snooping, broadcast storm control, IEEE802.1d/w spanning tree, port mirroring and so on.

1.1.2 Features and Benefits

- **MAC Address Control**

Besides the standard dynamic learning capability of MAC address, the SS2R24/48G4i switch also supports several other methods of management based on the MAC address list. The MAC address binding function can restrict the MAC addresses of access equipment connected to a port, in order to keep access secure. The MAC address filtering function can filter according to source and destination MAC addresses to block the invalid access equipment.

- **VLAN Configuration**

The switch supports standard IEEE802.1Q VLAN, port-protect VLAN and PVLAN. IEEE802.1 Q VLAN can divide ports into several VLAN groups, the upper limit of which is 4094. It can also do multi-switch VLAN division via IEEE802.1 Q VLAN, and thus manage to control broadcast traffic, guarantee the security and performance of the network at the same time. PVLAN function can divide ports into isolated port and community port, then isolate or connect ports as demanded by network applications.

- **QoS**

The switch fully supports QoS policy. Users can specify 4 priority queue on each port. WRR/SP/SWRR scheduling is also supported. SS2R24/48G4i switch also supports the port security. The traffic can be sorted by port, VLAN, DSCP, IP precedence and ACL table. User can also modify packets' DSCP and IP precedence values. Users can specify different bandwidths for voice/data/video to customize different qualities of service.

- **ACL**

The switch supports complete ACL policy. ACL is a mechanism realized by switches to filter IP data. By allowing or denying specific data packets entering/leaving the network, a switch can control the network access and effectively guarantee the secure operation of network. SS2R24/48G4i switch supports IP -based, MAC-based and MAC-IP-based ingress filtering, it can also filter data based on the information of source/destination IP address, source/destination MAC address, IP protocol type, TCP/UDP port, IP precedence, time range and ToS, etc..

- **IEEE802.1x Access Authentication**

The switch not only supports port-based IEEE802.1x authentication mode, but also supports MAC -based authentication mode. It can set the upper limit of access authentication users per port, realize dynamic secure authentication mode basing on MAC address, and bind the MAC address of an authenticated equipment to a port. Combining these IEEE802.1x authentication modes with the authentication and cost-counting products, we can supply a whole set of integrated IEEE802.1x access authentication and cost-counting resolution to satisfy the need of access, authentication and cost-counting, ensuring the network's security and its ability to operate.

- **Bandwidth Control (Speed Limit of Port)**

The switch can control the upstream/ downstream bandwidth and provide different access bandwidth for users of different levels. Each port can set its bandwidth rate as demanded to meet the need of access network to control access bandwidth.

- **TRUNK**

The switch supports IEEE802.3ad standard TRUNK. It can also realize link redundancy and traffic load balance.

- **IGMP Snooping**

The switch supports multicast applications which are based on IGMP Snooping mechanism, and as a result, it can realize all kinds of multicast services, diminish the network traffic and meet the requirement of multicast services like multimedia playing, remote teaching and entertainment.

- **Broadcast Storm Control**

The switch supports broadcast storm control, can effectively control broadcast storm, decrease useless occupancy of bandwidth, and increase the overall performance of network.

- **Spanning tree**

The switch supports IEEE802.1D spanning tree and IEEE802.1w rapid spanning tree. Spanning tree can effectively avoid loop, and at the same time, create a redundant backup for the link.

- **Port Image**

The switch supports port Image, which can mirror the inbound/outbound traffic of one or more ports to another port, in order to detect relative information of data. This function can be used to debug network faults and monitor traffic.

- **DHCP Server, Client**

The switch supports DHCP server, can dynamically allocate IP addresses for equipment, and bind MAC with IP by designating IP for a specified MAC.

- **RADIUS**

The switch supports RADIUS(Remote Authentication Dial In User Service). RADIUS allows users to authenticate identity via IEEE802.1x protocol.

- **Complete Network Management**

The switch can do out-of-band and in-band management via Console, Telnet, Web and SNMP. Console and Telnet management support standard CLI(Command Line Interface). Web management provides a remote browsing graphic management interface to make management more direct and convenient, to enable fast check of working state and to do real-time configuration management. SNMP management is in accordance with V1, V2C and V3 standard version, supporting Ether-Like MIB, Bridge MIB and MIB II, as well as standard management information libraries including RMON 1/2/3/9 MI etc.

The SS2R24/48G4i switch also supports SSH protocol to maximumly ensure the safety of configuration management. What's more, the SS2R24/48G4i switch provide an unique function to manage and set the IP of workstations, enabling the switch to automatically filter invalid remote network management access and guaranteeing the efficiency, security and coherence of remote network management access.

1.1.3 Main Features

- Applying Store-and-Forward switch mode to ensure block-free transmission.
- All of the RJ-45 ports support MDI/MDI-X self-adaptation, can be conveniently cascade connected to other switcher using straight-through twisted pair.
- Providing Console port.
- Allowing users to check the working state and statistic information of ports.
- Can be rebooted locally and remotely to reset the switch to the default configuration.

- Can update the firmware using TFTP/FTP.
- Can be fixed in a standard 19-inch frame.

1.2 Technical specifications

- **Protocols and Standards**
  - IEEE802.3 10BASE-T Ethernet
  - IEEE802.3u 100BASE-TX/FX Fast Ethernet
  - IEEE802.3x Flow control
  - IEEE802.1x access control
  - IEEE802.1D/w Spanning Tree
  - IEEE802.1p Class of Service
  - IEEE802.1Q VLAN
  - IEEE802.3ad Link Aggregation
  - TFTP/FTP
  - DHCP
  - BootP
  - Telnet
  - IP/UDP/TCP/ICMP
  - HTTP
  - SNMP V1/V2C

- **Management Protocols and Methods**
- CLI command line
  - SNMP V1/V2C enabled, available through Network management systems such as LinkManager
  - Web and Telnet management enable
  - RFC1757 RMON(1、2、3、9)

- **MIB Library**
  - RFC1213 MIB II
  - RFC1493 Bridge MIB
  - RFC1643 Ether-Like MIB
  - Private MIB

■ **Management Protocols and Methods**

☐ CLI command line

☐ SNMP V1/V2C enabled, available through Network management systems such as LinkManager

☐ Telnet management enabled

☐ RFC1757 RMON(1, 2, 3, 9)

■ **MIB Library**

a) RFC1213 MIB II

b) RFC1493 Bridge MIB

c) RFC1643 Ether-Like MIB

d) Private MIB

1.3 Physical Specifications

	SS2R24G4I/SS2R48G4I	SS2R48G4I/52C
weight	2.25KG	3KG
Dimension (mm)	440×171.2×43	440×229×44
Operating Temperature	0°C～50°C	
Storage Temperature	-40°C～70°C	
Relative humidity	10%～90%，with no condensate	
AC Power Input	100～240VAC，50～60Hz	
Power Consumption	30W Max	
Mean Time Before Failure	80,000 Hours	

Table1-1 SS2R24/48G4i switch switch physical specification

1.4 Product appearance

1.4.1 Product Front Panel View

SS2R24/48G4i switch switch front panel view as follows

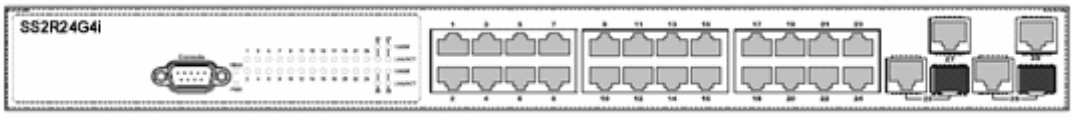


Fig 1-3 SS2R24G4i switch front panel view

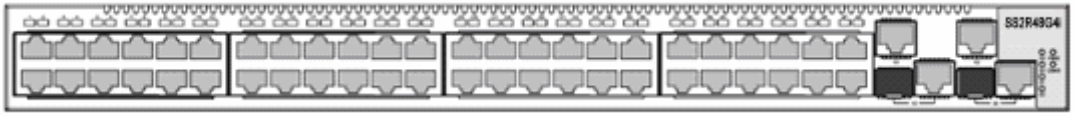


Fig 1-4 SS2R48G4i switch front panel view

1.4.2 Product back panel view

SS2R24/48G4i switch back panel view as follows

Fig 1-5 SS2R24G4i back panel view

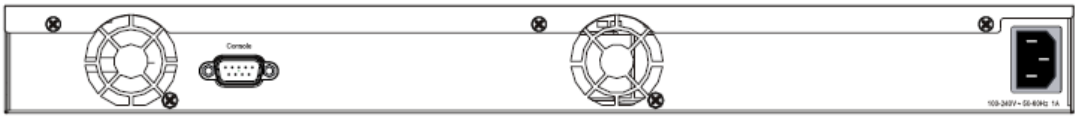


Fig 1-6 SS2R48G4i back panel view

1.4.3 Status LEDs

The LEDs of SS2R24/48G4i switch switch include PWR, DIAG, Link/Act and 1000M. The LEDs are located on the front panel for easy viewing and shown below

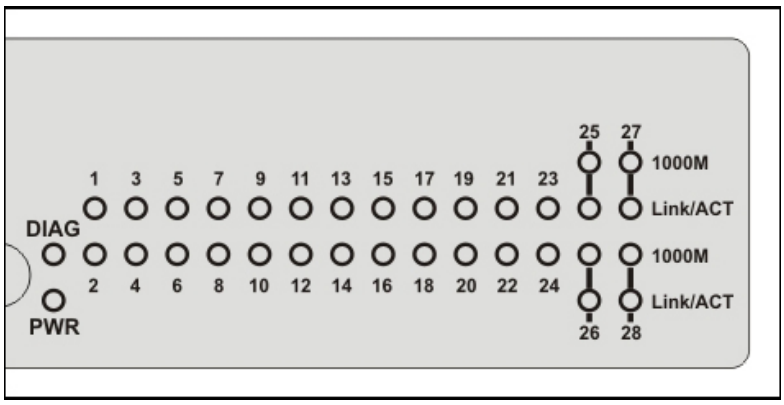


Fig 1-7 SS2R24G4i switch LEDs

Description of LEDs

LED	Sstate	Description
Link/ACT	Blink	The port is successfully linked and is sending /receiving data right now.
	Off	The state of the port is down.
	On	Link succeeds
1000M indicator lamp	On	The corresponding G port is in 1000M connecting mode.
	Off	The corresponding G port is in 100M connecting mode or in down state.
Power	On	Power on
	Off	Power off

DIAG	Green,blink	The program is initializing.
	On	The program has been initialized successfully.
	yellow,blink	The initialization of the program has failed.

Table1-2 Description of LEDs in SS2R24G4i/SS2R48G4i Switch

SS2R48G4iswitch does not have the 1000M LED. The Link/ACT LED of its 100M port is above the corresponding port, while the Link/ACT iLED of its 1000M port is on the right of the corresponding port.

Chapter 2 Hardware Installation

2.1 Installation Notice

To ensure the proper operation of SS2R24/48G4i switch and your physical security, please read carefully the following installation guide.

2.1.1 Environmental Requirements

- The switch must be installed in a clean area. Otherwise, the switch may be damaged by electrostatic adherence.
- Maintain the temperature within 0 to 50 °C and the humidity within 5% to 95%, non-condensing.
- The switch must be put in a dry and cool place. Leave sufficient spacing around the switch for good air circulation.
- The switch must work in the right range of power input AC power 100 ~ 240VAC (50 ~ 60Hz).
- The switch must be well grounded in order to avoid ESD damage and physical injury of people.
- The switch should avoid sunlight perpendicular incidence. Keep the switch away from heat sources and strong electromagnetic interference sources.
- The switch must be mounted to a standard 19" rack or placed on a clean level desktop.

2.1.1.1 Dust and Particles

Dust is harmful to the safe operation of SS2R24/48G4i switch. Dust can lead to electrostatic adherence, especially likely under low relative humidity, causing poor contact of metal connectors or contacts. Electrostatic adherence will result in not only reduced product lifespan, but also increased chance of communication failures. The recommended value for dust content and particle diameter in the site is shown below

Max Diameter (μm)	0.5	1	3	5
Max Density (particles/m³)	1.4×10^7	7×10^5	2.4×10^5	1.3×10^5

Table 2-1 Environmental Requirements Dust

In addition, salt, acid and sulfide in the air are also harmful to the switch. Such harmful gases will aggravate metal corrosion and the aging of some parts. The site should avoid harmful gases, such as SO_2, H_2S, NO_2, NH_3 and Cl_2, etc. The table below details the threshold value.

Gas	Average (mg/m³)	Max (mg/m³)
SO_2	0.2	1.5
H_2S	0.006	0.03
NO_2	0.04	0.15

NH_3	0.05	0.15
Cl_2	0.01	0.3

Table 2-2 Environmental Requirements Particles

2.1.1.2 Temperature and Humidity

As the switch is designed to no fan, it's physical heat-away ,the site should still maintain a desirable temperature and humidity. High-humidity conditions can cause electrical resistance degradation or even electric leakage, degradation of mechanical properties and corrosion of internal components. Extreme low relative humidity may cause the insulation spacer to contract, making the fastening screw insecure. Furthermore, in dry environments, static electricity is liable to be produced and cause harm to internal circuits. Temperature extremes can cause reduced reliability and premature aging of insulation materials, thus reducing the switch's working lifespan. In the hot summer, it is recommended to use air-conditioners to cool down the site. And the cold winter, it is recommenced to use heaters.

The recommended temperature and humidity is shown below

Temperature		**Relative humidity**	
Long term condition	Short term condition	Long term condition	Short term condition
15 ~ 30°C	0 ~ 50°C	40 ~ 65%	10 ~ 95%

Table 2-3 Environmental Requirements Temperature and Humidity

Caution !!

A sample of ambient temperature and humidity should be taken at 1.5m above the floor and 0.4m in front of the switch rack, with no protective panel covering the front and rear of the rack.

Short term working conditions refer to a maximum of 48 hours of continued operation and an annual cumulative total of less than 15 days. Formidable operation conditions refers to the ambient temperature and relative humidity value that may occur during an air-conditioning system failure, and normal operation conditions should be recovered within 5 hours.

2.1.1.3 Power Supply

SS2R24/48G4i switch is designed to use modular switching power supplies. The power input specification is shown below

Nominal Input Voltage AC 100 ~ 240 VAC,

Frequency 50-60Hz

Total power consumption ≤30W

Before powering on the power supply, please check the power input to ensure proper grounding of the power supply system. The input source for the switch should be reliable and secure, a voltage adaptor can be used if necessary. The building's circuit protection system should include in the circuit a fuse or circuit-breaker of no greater than 240 V, 10 A. It is recommended to use a UPS for more reliable power supplying

Caution !!

Improper power supply system grounding, extreme fluctuation of the input source and transients (or spikes) can result in larger error rate, or even hardware damage!

2.1.1.4 Preventing Electrostatic Discharge Damage

Static electric discharges can cause damage to internal circuits, even the entire switch. Follow these guidelines for avoiding ESD damage

- Ensure proper earth grounding of the device
- Perform regular cleaning to reduce dust
- Maintain proper temperature and humidity
- Always wear an ESD wrist strap and antistatic uniform when in contact with circuit boards

2.1.1.5 Anti-interference

All sources of interference, whether from the device/system itself or the outside environment, will affect operations in various ways, such as capacitive coupling, inductive coupling, electromagnetic radiation, common impedance (including the grounding system) and cables/lines (power cables, signal lines, and output lines). The following should be noted

- Precautions should be taken to prevent power source interruptions
- Provide the system with a dedicated grounding, rather than sharing the grounding with the electronic equipment or lightning protection devices
- Keep away from high power radio transmitters, radar transmitters, and high frequency strong circuit devices
- Provide electromagnetic shielding if necessary

2.1.1.6 Rack Configuration

The dimensions of the switch designed to be mounted on a standard 19’’ rack, Please ensure good ventilation for the rack

- Every device in the rack will generate heat during operation, therefore vent and fans must be provided for an enclosed rack, and devices should not be stacked closely.
- When mounting devices in an open rack, care should be taken to prevent the rack frame from obstructing the switch ventilation openings. Be sure to check the positioning of the switch after installation to avoid the aforementioned.

Caution !!

If a standard 19’’ rack is not available, the switch can be placed on a clean level desktop, leave a clearance of 10mm around the switch for ventilation, and do not place anything on top of the switch

---

2.1.2 Installation Notice

- Read through the installation instruction carefully before operating on the system. Make sure the

installation materials and tools are prepared. And make sure the installation site is well prepared.

- During the installation, users must use the brackets and screws provided in the accessory kit. Users should use the proper tools to perform the installation. Users should always wear antistatic uniform and ESD wrist straps. Users should use standard cables and connecters.
- After the installation, users should clean the site. Before powering on the switch, users should ensure the switch is well grounded. Users should maintain the switch regularly to extend the lifespan of the switch.

2.1.3 Security Warnings

- When using SFP transceiver, do not stare directly at the fiber bore when the switch is in operation. Otherwise the laser may hurt your eyes.
- Do not attempt to conduct the operations which can damage the switch or which can cause physical injury.
- Do not install, move or disclose the switch and its modules when the switch is in operation.
- Do not open the switch shell.
- Do not drop metals into the switch. It can cause short-circuit.
- Do not touch the power plug and power socket.
- Do not place the tinder near the switch.
- Do not configure the switch alone in a dangerous situation.
- Use standard power sockets which have overload and leakage protection.
- Inspect and maintain the site and the switch regularly.
- Have the emergence power switch on the site. In case of emergence, switch off the power immediately.

2.2 Installation Preparation

2.2.1 Verify the Packet Contents

The above contents are subject to the received packet contents.

2.2.2 Required Tools and Utilities

The required tools and utilities	● Cross screwdrivers
	● Flat-blade screwdriver
	● wire clamp
	● Antistatic uniform
	● ESD wrist strap
	● Antistatic glove
Connecting cable	● Console cable and commutator
	● Standard Twisted-pair

	● RJ-45 pin

Table 2-4 The required tools and utilities

2.3 Hardware Installation

2.3.1 Installing the Switch

Please mount SS2R24/48G4i switch on the 19'' rack as below

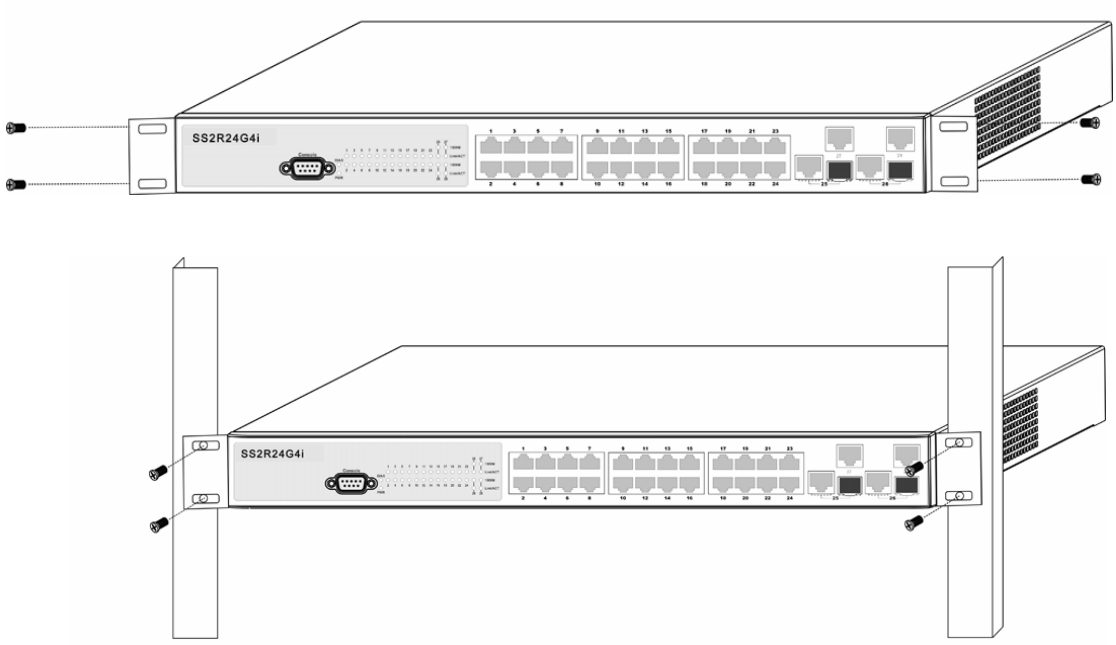


Fig 2-1 SS2R24/48G4i switch Rack-mounting

1. Attach the 2 brackets on the SS2R24/48G4i switch with screws provided in the accessory kit.
2. Put the bracket-mounted switch smoothly into a standard 19'' rack. Fasten the SS2R24/48G4i switch to the rack with the screws provided. Leave enough space around the switch for good air circulation.

Caution!

The brackets are used to fix the switch on the rack. They can't serve as a bearing. Please place a rack shelf under the switch. Do not place anything on top of the switch. Do not block the blowholes on the switch to ensure the proper operation of the switch.

2.3.2 Connecting Console

SS2R24/48G4i switch provides a DB9 interface serial console port. The connection procedure is

listed below

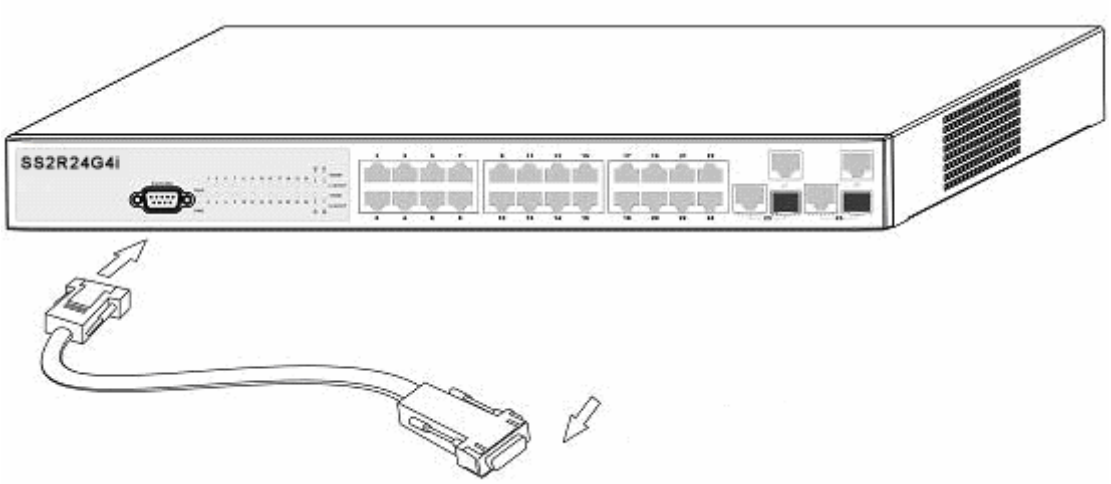


Fig 2-2 Connecting Console to SS2R24/48G4i switch

1. Find the console cable provided in the accessory kit. Attach the Mini-USB end to console port of the switch.
2. Connect the other side of the console cable to a character terminal (PC).
3. Power on the switch and the character terminal. Configure the switch through the character terminal.

Caution!

Please use the console cable and the console commutator of the switch.Don't insert in error to avoid break.

2.3.3 Power Supply Connection

SS2R24/48G4i switch uses 100～240VAC,50～60Hz supply by default. AC Power supply connection procedure is described as below

1. Insert one end of the power cable provided in the accessory kit into the power source socket (with overload and leakage protection), and the other end to the power socket in the back panel of the switch.
2. Check the power status indicator in the front panel of the switch. The corresponding power indicator should light. SS2R24/48G4i switch is self-adjustable for the input voltage. As soon as the input voltage is in the range printed on the switch surface, the switch can operate correctly.
3. When the switch is powered on, it executes self-test procedure and startups.

Caution!

The input voltage must be within the required range, otherwise the switch could malfunction of be damaged. Do not open the switch shell without permission. It can cause physical injury

---

Chapter 3 Setup Configuration

Setup configuration refers to the initial operation to the switch after the user purchases the switch. For first-time users of the SS2R24/48G4i switch, this chapter provides a very practical instruction. When using the CLI (command line interface), the user can type *setup* under admin mode to enter the Setup configuration interface.

3.1 Setup Configuration

Setup configuration is done via menu selections, in which switch hostname, Vlan1 interface, Telnet service, Web service,and SNMP, can be configured.

3.2 Main Setup Menu

Before entry into the main menu, the following screen will be displayed to prompt the user to select a preferred interface language. English users should choose “0” to enter the English interface, while Chinese users can choose “1” to view the interface in Chinese.

Please select language
[0] English
[1] Chinese
Selection(0|1)[0]

The main Setup configuration menu is listed below

Configure menu
[0] Config hostname
[1] Config interface-Vlan1
[2] Config telenet-server
[3] Config web-server
[4] Config SNMP
[5] Exit setup configuration without saving
[6] Exit setup configuration after saving
Selection number

3.3 Setup Submenu

3.3.1 Configuring switch hostname

Select “0” in the Setup main menu and press Enter, the following screen appears

Please input the host name[switch]

Note the hostname entered should be less than 30 characters. If the user presses Enter without input, the hostname will default to “switch”

3.3.2 Configuring Vlan1 Interface

Select “1” in the Setup main menu and press Enter to start configuring the Vlan1 interface

Config Interface-Vlan1

[0] Config interface-Vlan1 IP address

[1] Config interface-Vlan1 status

[2] Exit

Selection number

Select “0” in the Vlan1 interface configuration menu and press Enter, the following screen appears

Please input interface-Vlan1 IP address (A.B.C.D)

When the user enters valid IP address for Vlan1 interface and presses Enter, the following screen will appear

Please input interface-Vlan1 mask [255.255.255.0]

Select “1” in the Vlan1 interface configuration menu and press Enter, the following screen will appear

Open interface-Vlan1 for remote configuration ? (y/n) [y]

Select “2” in the Vlan1 interface configuration menu will return to the Setup main menu.

3.3.3 Telnet Server Configuration

Select “2” in the Setup main menu and press Enter to start configuring the Telnet server, the follow appears

Configure telnet server

[0] Add telnet user

[1] Config telnet server status

[2] Exit

Selection number

Select “0” in the Telnet server configuration menu and press Enter, the following screen appears

Please input the new telnet user name

Note the valid username length is 1 to 16 characters. When the user enters a valid username and presses Enter, the following screen appears

Please input the new telnet user password

Select “1” in the Telnet server configuration menu and press Enter, the following screen appears

Enable switch telnet-server or no?(y/n) [y]

Type “y” and press Enter, or just press Enter to enable Telnet service, type “n” and press Enter to disable Telnet service. The Telnet server configuration menu appears.

Select “2” in the Telnet server configuration menu will return to the Setup main menu.

3.3.4 Configuring Web Server

Select “3” in the Setup main menu and press Enter to start configuring the Web server, the follow appears

Configure web server
[0] Add webuser
[1] Config web server status
[2] Exit
Selection number

Select “0” in the Web server configuration menu and press Enter, the following screen appears
Please input the new web user name

Note the valid username length is 1 to 16 characters. When the user enters a valid username and presses Enter, the following screen appears
Please input the new web user password

Note the valid password length is 1 to 8 characters. After configuring the username and password, the menu will return to the Web server configuration section

Select “1” in the Web server configuration menu and press Enter, the following screen appears
Enable switch web-server or no?(y/n) [y]
Type “y” and press Enter, or just press Enter to enable Web service, type “n” and press Enter to disable Web service. The Web server configuration menu appears.

Select “2” in the Telnet server configuration menu will return to the Setup main menu.

3.3.5 Configuring SNMP

Select “4” in the Setup main menu and press Enter to start configuring SNMP, the following appears

Configure SNMP
[0] Config SNMP-server read-write community string
[1] Config SNMP-server read-only community string
[2] Config traps-host and community string
[3] Config SNMP-server status
[4] Config SNMP traps status
[5] Add SNMP NMS security IP address
[6] Exit
Selection number

Select “0” in SNMP configuration menu and press Enter, the following screen appears

Please input the read-write access community string[private]

Note the valid length for a read-write access community string is 1 to 255 characters, the default value is “private”. When a valid read-write access community string is entered, pressing Enter returns you to the SNMP configuration menu.

Select “1” in the SNMP configuration menu and press Enter, the following screen will appear

Please input the read-only access community string[public]

Note the valid length for a read-only access community string is 1 to 255 characters, the default value is “public”. When a valid read-only access community string is entered, press Enter returns to the SNMP configuration menu.

Select “2” in the SNMP configuration menu and press Enter, the following screen will appear

Please input traps-host IP address(A.B.C.D)

When the user enters a valid IP address for Traps host and presses Enter, the following appears

Please input traps community string[public]

Note the valid length for a traps community string is 1 to 255 characters, the default value is “public”. When a valid traps community string is entered, press Enter returns to the SNMP configuration menu.

Select “3” in the SNMP configuration menu and press Enter, the following screen will appear

Enable SNMP-server? (y/n) [y]

Type “y” and press Enter, or just press Enter to enable SNMP service, type “n” and press Enter to disable SNMP service. The SNMP configuration menu appears.

Select “4” in the SNMP configuration menu and press Enter, the following screen will appear

Enable SNMP-traps ? (y/n) [y]

Type “y” and press Enter, or just press Enter to enable SNMP Traps, type “n” and press Enter to disable SNMP traps. The SNMP configuration menu appears.

Select “5” in the SNMP configuration menu and press Enter, the following screen appears

Please input the new NMS IP address(A.B.C.D)

When a valid secure IP address(es) for SNMP management workstation is entered, press Enter to return to the SNMP configuration menu.

Selecting “6” in the SNMP configuration menu will return to the Setup main menu.

3.3.6 Exiting Setup Configuration Mode

Select “5” in the Setup main menu to exit the Setup configuration mode without saving the configurations made.

Selecting “6” in the Setup main menu exits the Setup configuration mode and saves the configurations made. This is equivalent to running the *Write* command. For instance, if under the Setup configuration mode, the user sets a Telnet user and enables Telnet service, and selects “5” to exit Setup main menu. He/She will be able to configure the switch through Telnet from a terminal.

When exiting the Setup configuration mode, the CLI configuration interface appears. Configuration commands and syntaxes will be described in detail in later chapters.

Chapter 4 Switch Management

4.1 Management Options

After purchasing the switch, the user needs to configure the switch for network management. SS2R24/48G4i switch provides two management options in-band management and out-of-band management.

4.1.1 Out-of-band Management

Out-of-band management is the management through Console interface. Generally, the user will use out-of-band management for the initial switch configuration, or when in-band management is not available. For instance, the user must assign an IP address to the switch via the Console interface to be able to access the switch through Telnet.

The procedures for management via Console interface are listed below

Step 1　setting up the environment

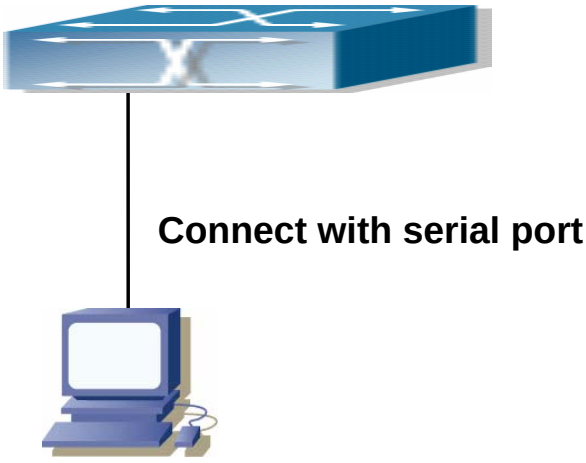


Fig 4-1 Out-of-band Management Configuration Environment

the serial port (RS-232) is connected to the switch with the serial cable provided. The table below lists all the devices used in the connection.

Device Name	Description
PC machine	Has functional keyboard and RS-232, with terminal emulator installed, such as the HyperTerminal included in Windows 9x/NT/2000/XP.
Serial port cable	One end attach to the RS-232 serial port, the other end to the Console port of SS2R24/48G4i switch.
The switch	Functional Console port required.

Step 2　Entering HyperTerminal.

Open the HyperTerminal included in Windows after the connection established.

1) Click Start menu - All Programs – Accessories – Communication - HyperTerminal.

2)Type a name for opening HyperTerminal, such as “Switch_A”.

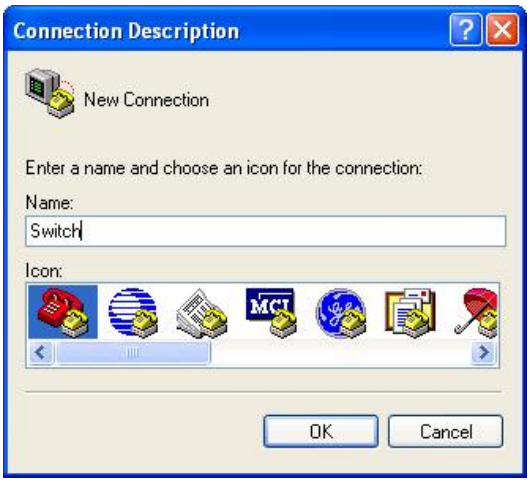


Fig 4-2 Opening HyperTerminal

3)In the “Connecting with” drop-list, select the RS-232 serial port used by the PC, e.g. COM1, and click “OK”.

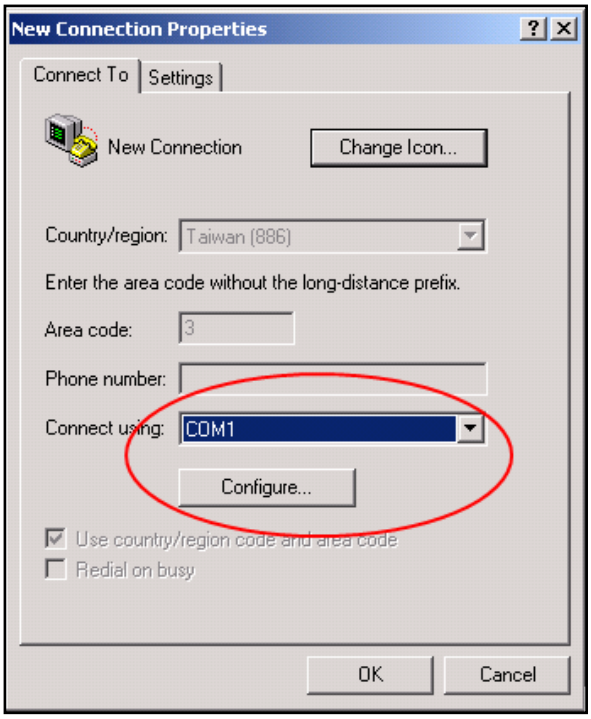


Fig 4-3 Opening HyperTerminal

4)COM1 property appears, select “9600” for “Baud rate”, “8” for “Data bits”, “none” for “Parity checksum”, “1” for stop bit and “none” for traffic control; or, you can also click “Revert to default” and click “OK”.

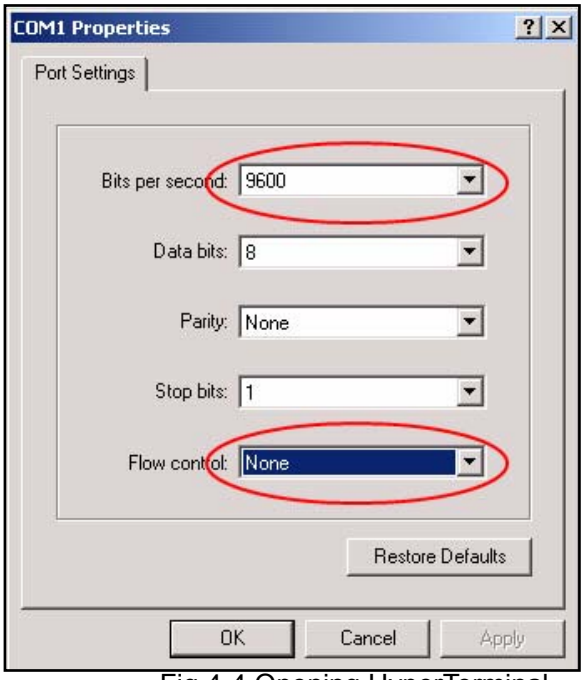


Fig 4-4 Opening HyperTerminal

Step 3 Entering switch CLI interface

```
Power on the switch. The following appears in the HyperTerminal windows,
that is the CLI configuration mode for
Testing RAM...
67,108,864 RAM OK.

Initializing...

Booting......
Starting at 0x10000...

Current time is MON JAN 01 00 00 00 2001

SS2R24G4I Series Switch Operating System
SoftWare Version RS-5200-28_1.2.17.0
NOS Version NOS_5.1.35.47
Copyright (C) 2001-2007 AMER. COM
http //www.amer.com

SS2R24G4I Switch (88E6218-133M) processor
28 Ethernet/IEEE 802.3 interface(s)
Switch>
```

The user can now enter commands to manage the switch. For a detailed description for the commands, please refer to the following chapters.

4.1.2 In-band Management

In-band management refers to the management by logging into the switch using Telnet. In-band management enables the function of managing the switch for some devices attached to the switch. In the case when in-band management fails due to switch configuration changes, out-of-band management can be used for configuring and managing the switch.

4.1.2.1 Management via Telnet

To manage the switch with Telnet, the following conditions should be met

1) Switch has an IP address configured;
2) The host IP address (Telnet client) and the switch's VLAN interface IP address is in the same network segment.
3) If not 2), Telnet client can connect to an IP address of the switch via other devices, such as a router.

SS2R24/48G4i switch are Layer 2 switch that can be configured with several IP addresses. The following example assumes the shipment status of the switch, where only VLAN1 exists in the system.

The following describes the steps for a Telnet client to connect to the switch's VLAN1 interface by Telnet.

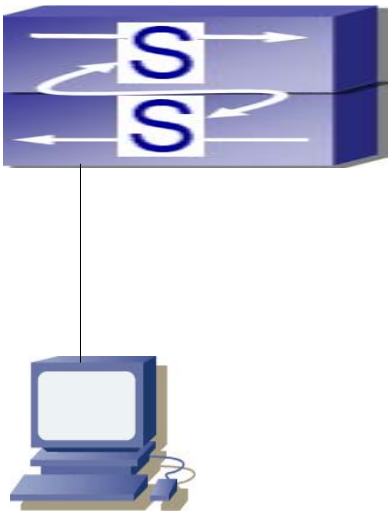


Fig 4-5 Manage the switch by Telnet

Step 1 Configure the IP addresses for the switch

First is the configuration of host IP address, which should be within the same network segment as the switch VLAN1 interface IP address. Suppose the switch VLAN interface IP address 10.1.128.251/24, then a possible host IP address is 10.1.128.25/24. Run "ping 10.1.128.251" from the host and verify the result, check for reasons if ping fails.

The IP address configuration commands for VLAN1 interface SS2R24/48G4i switch are listed

below. Before in-band management, the switch must be configured with an IP address by out-of-band management (i.e. Console mode), The configuration commands (All switch configuration prompts are assumed to be “switch” hereafter if not otherwise specified)

Switch>
Switch>en
Switch#config
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.128.251 255.255.255.0
Switch(Config-If-Vlan1)#no shutdown

Step 2 Run Telnet Client program

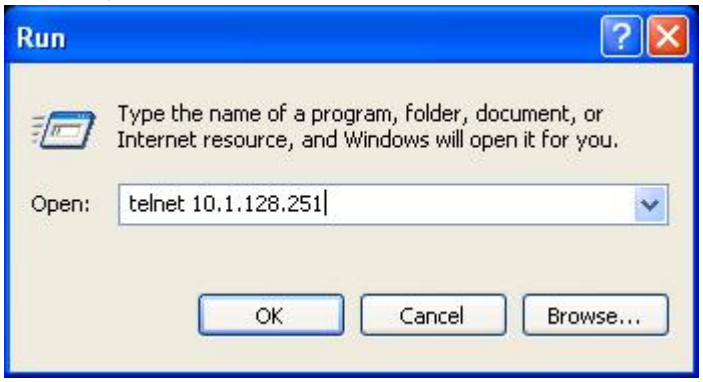


Fig 4-6 Run telnet client program included in Windows

Run Telnet client program included in Windows with the specified Telnet target

Step 3 Login to the switch

Login in to the Telnet configuration interface. Valid login name and password is required, otherwise the switch will reject Telnet access. This is a method to protect the switch from unauthorized access. If no authorized Telnet user has been configured, nobody can connect to the Telnet CLI configuration interface. As a result, when Telnet is enabled for configuring and managing the switch, username and password for authorized Telnet users must be configured with the following command

telnet-user <user> password {0|7} <password>

Assume a authorized user in the switch has a username of “test”, and password of “test”, the configuration procedure should be like the following

Switch>en
Switch#config
Switch(Config)#telnet-user test password 0 test

Enter valid login name and password in the Telnet configuration interface, Telnet user will be able to enter the switch’s CLI configuration interface. The commands used in the Telnet CLI interface after login are the same as in that in the Console interface.

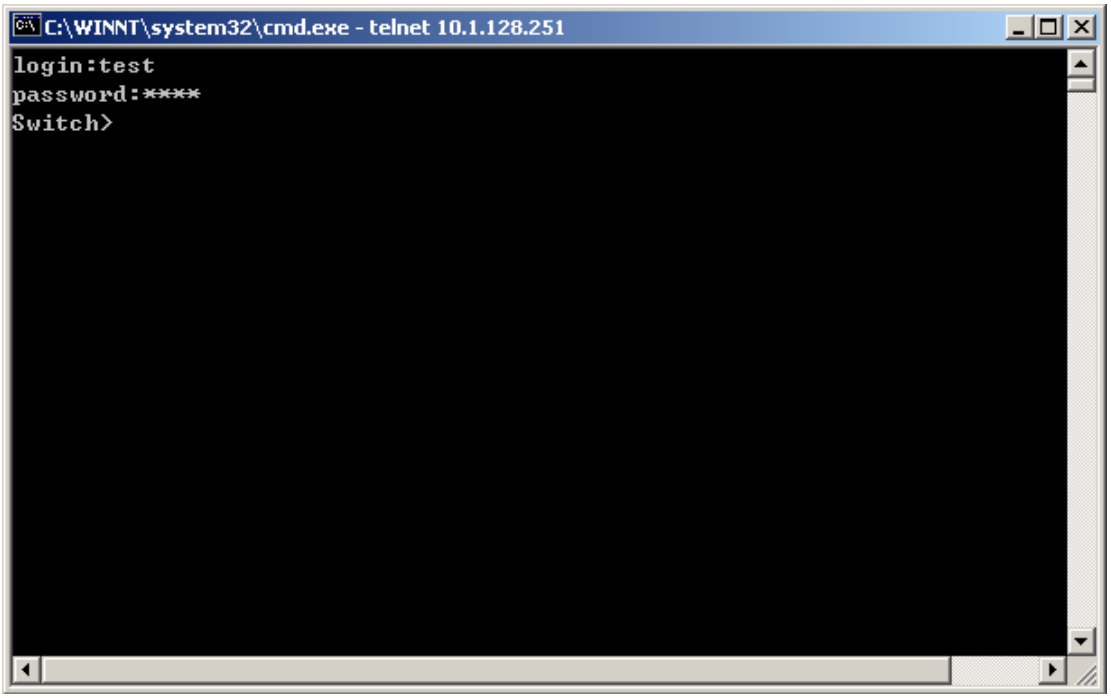


Fig 4-7 Telnet Configuration Interface

4.1.2.2 Management via HTTP

To manage the switch via HTTP, the following conditions should be meet

1) Switch has an IP address configured;
2) The host IP address and the switch's VLAN interface IP address is in the same network segment.
3) If not 2), Telnet client can connect to an IP address of the switch via other devices, such as a router.

Similar to management via Telnet, as soon as the host succeeds to ping an IP address of the switch and to type the right login password, it can access the switch via HTTP. The configuration list is as below

Step 1 Configure the IP addresses for the switch and start the HTTP function on the switch.

For configuring the IP address on the switch through out-of-band management, see the relevant chapter.

To enable the WEB configuration, users should type the CLI command **ip http server** in the global mode as below

Switch>en
Switch#config
Switch(Config)#ip http server

Step 2 Run HTTP protocol on the host.

Open the Web browser on the host and type the IP address of the switch.Or run directly the HTTP protocol on the Windows. For example, the IP address of the switch is "10.1.128.251".

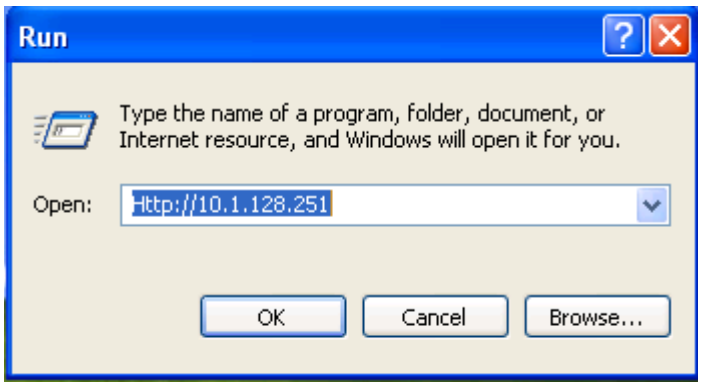


Fig 4-8 Run HTTP Protocol

Step 3 Logon to the switch

To logon to the HTTP configuration interface, valid login user name and password are required; otherwise the switch will reject HTTP access. This is a method to protect the switch from the unauthorized access. Consequently, in order to configure the switch via HTTP, username and password for authorized HTTP users must be configured with the following command in the global mode

web-user <*user*> password {0|7} <*password*> Suppose an authorized user in the switch has a username as “test”, and password as “test”. The configuration procedure is as below

Switch>en
Switch#config
Switch(Config)#web-user admin password 0 digital
Input the right username and password, and then the main Web configuration interface

4.1.2.3 Management via LinkManager

To manage the switch with LinkManager, the following conditions should be met

1) Switch has an IP address configured
2) The host IP address (LinkManager) and the switch’s VLAN interface IP address is in the same network segment.
3) If not 2), LinkManager can connect to an IP address of the switch via other devices, such as a router.

Management via LinkManager, the host succeeds to ping an IP address of the switch,then run the switch, LinkManager network management software will be found by SS2R24/48G4i switch,and operate it with read-write permission

4.2 Management Interface

SS2R24/48G4i switch provide three management interfaces CLI(Command Line Interface), Web interface, LinkManager network management software

4.2.1 CLI Interface

CLI interface is familiar to most users. As aforementioned, out-of-band management and Telnet login are all performed through CLI interface to manage the switch.

CLI Interface is supported by Shell program, which consists of a set of configuration commands. Those commands are categorized according to their functions in switch configuration and management. Each category represents a different configuration mode. The Shell for the switch is described below

- Configuration Modes
- Configuration Syntax
- Shortcut keys
- Help function
- Input verification
- Fuzzy match support

4.2.1.1 Configuration Modes

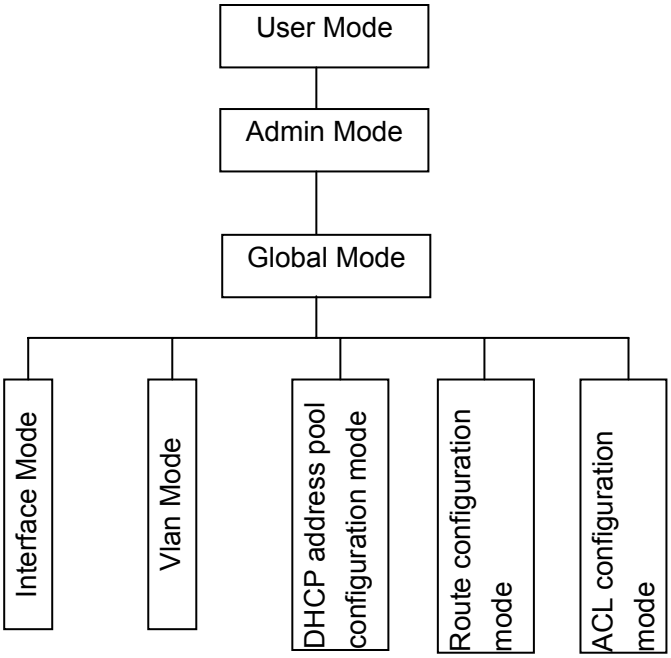


Fig 4-9 Shell Configuration Modes of SS2R24/48G4i switch

4.2.1.1.1 User Mode

On entering the CLI interface, entering user entry system first. If as common user, it is defaulted to User Mode. The prompt shown is "**Switch**>", the symbol ">" is the prompt for User Mode. When **exit** command is exit under Admin Mode, it will also return to the User Mode.

Under User Mode, no configuration to the switch is allowed, only clock time and version information of the switch can be queries.

4.2.1.1.2 Admin Mode

When **enable** command is used under User Mode,To Admin Mode sees the following In user entry system, if as Admin user, it is defaulted to Admin Mode. Admin Mode prompt "**Switch#**" can be entered under the User Mode by running the *enable* command and entering corresponding access levels admin user password, if a password has been set. Or, when ***exit*** command is run under Global Mode, it will also return to the Admin Mode. SS2R24/48G4i switch Switch also provides a shortcut key sequence "Ctrl+z", this allows an easy way to exit to Admin Mode from any configuration mode (except User Mode).

Under Admin Mode, the user can query the switch configuration information, connection status and traffic statistics of all ports; and the user can further enter the Global Mode from Admin Mode to modify all configurations of the switch. For this reason, a password must be set for entering Admin mode to prevent unauthorized access and malicious modification to the switch.

4.2.1.1.3 Global Mode

Type the config command under Admin Mode will enter the Global Mode prompt "Switch(Config)**#**". Use the *exit* command under other configuration modes such as Interface Mode, VLAN mode will return to Global Mode.

The user can perform global configuration settings under Global Mode, such as MAC Table, Port Mirroring, VLAN creation, IGMP Snooping start, GVRP and STP, etc. And the user can go further to Interface Mode for configuration of all the interfaces.

4.2.1.1.4 Interface Mode

Use the ***interface*** command under Global Mode can enter the interface mode specified. SS2R24/48G4i switch Switch provides three interface type VLAN interface, Ethernet port and port-channel, and accordingly the three interface configuration modes.

Interface Type	**Entry**	**Prompt**	**Operates**	**Exit**
VLAN Interface	Type **interface vlan <Vlan-id>** command under Global Mode.	**Switch(Config-If-Vlanx)#**	Configure switch IPs, etc	Use the *exit* command to return to Global Mode.
Ethernet Port	Type **interface ethernet <interface-list>** command under Global Mode.	**Switch(Config-ethernetxx)#**	Configure supported duplex mode, speed, etc. of Ethernet Port.	Use the *exit* command to return to Global Mode.
port-channel	Type **interface port-channel**	**Switch(Config-if-port-channelx)#**	Configure port-channel	Use the *exit* command to

	<port-channel-number> command under Global Mode.		related settings such as duplex mode, speed, etc.	return to Global Mode.

4.2.1.1.5 VLAVLAN Mode

Using the ***vlan*** **<vlan-id>** command under Global Mode can enter the corresponding VLAN Mode. Under VLAN Mode the user can configure all member ports of the corresponding VLAN. Run the exit command to **exit** the VLAN Mode to Global Mode

4.2.1.1.6 DHCP Address Pool Mode

Type the **ip dhcp pool <*name*>** command under Global Mode will enter the DHCP Address Pool Mode prompt "**Switch(Config-<name>-dhcp)#**". DHCP address pool properties can be configured under DHCP Address Pool Mode. Run the *exit* command to exit the DHCP Address Pool Mode to Global Mode.

4.2.1.1.7 ACL Mode

ACL type	Entry	Prompt	Operates	Exit
Standard IP ACL Mode	Type **ip access-list standard** command under Global Mode.	**Switch(Config-Std-Nacl-a)#**	Configure parameters for Standard IP ACL Mode	Use the "*exit*" command to return to Global Mode.
Extended IP ACL Mode	Type **ip access-list extanded** command under Global Mode.	**Switch(Config-Ext-Nacl-b)#**	Configure parameters for Extended IP ACL Mode	Use the "*exit*" command to return to Global Mode.

4.2.1.2 Configuration Syntax

SS2R24/48G4i switch Switch provides various configuration commands. Although all the commands are different, they all abide by the syntax for SS2R24/48G4i switch Switch configuration commands. The general commands format of SS2R24/48G4i switch Switch is shown below

cmdtxt <*variable*> { enum1 | … | enumN } [option]

Conventions **cmdtxt** in bold font indicates a command keyword; **<*variable*>** indicates a variable

parameter; **{enum1 | … | enumN }** indicates a mandatory parameter that should be selected from the parameter set **enum1~enumN**; and the square bracket ([ ]) in **[option]** indicate an optional parameter. There may be combinations of "< >", "{ }" and "[ ]" in the command line, such as **[<*variable*>]**,**{enum1 <*variable*> | enum2}**, **[option1 [option2]], etc.**

Here are examples for some actual configuration commands

- **show version**， no parameters required. This is a command with only a keyword and no parameter, just type in the command to run.
- **vlan <*vlan-id*>**， parameter values are required after the keyword.
- **speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | {{force1g-half | force1g-full} [nonegotiate [master | slave]] } }**，the followings are possible
  speed-duplex auto
  speed-duplex force10-half
  speed-duplex force10-full
  speed-duplex force100-half
  speed-duplex force100-full
  speed-duplex force1g-half
  speed-duplex force1g-half nonegotiate
  speed-duplex force1g-half nonegotiate master
  speed-duplex force1g-half nonegotiate slave
  speed-duplex force1g-full
  speed-duplex force1g-full nonegotiate
  speed-duplex force1g-full nonegotiate master
  speed-duplex force1g-full nonegotiate slave

- **snmp-server community {ro|rw} <*string*>**， the followings are possible
  snmp-server community ro <*string*>
  snmp-server community rw <*string*>

4.2.1.3 Shortcut Key Support

SS2R24/48G4i switch switch provides several shortcut keys to facilitate user configuration, such as up, down, left, right and Blank Space. If the terminal does not recognize Up and Down keys, ctrl +p and ctrl +n can be used instead.

Key(s)	**Function**	
Back Space	Delete a character before the cursor, and the cursor moves back.	
Up "↑"	Show previous command entered. Up to ten recently entered commands can be shown.	
Down "↓"	Show next command entered. When use the Up key to get previously entered commands, you can use the Down key to return to the next command	
Left "←"	The cursor moves one character to the left.	You can use the Left and Right key to modify an

Right “→”	The cursor moves one character to the right.	entered command.
Ctrl +p	The same as Up key “↑”.	
Ctrl +n	The same as Down key “↓”.	
Ctrl +b	The same as Left key “←”.	
Ctrl +f	The same as Right key “→”.	
Ctrl +z	Return to the Admin Mode directly from the other configuration modes (except User Mode).	
Ctrl +c	Break the ongoing command process, such as ping or other command execution.	
Tab	When a string for a command or keyword is entered, the Tab can be used to complete the command or keyword if there is no conflict.	
/	Perform command of previous list,such as perform show command of admin mode under config mode Switch(Config)#/show run	
//	Perform command of previous list,such as perform show command of admin mode under port config Switch(Config-Port-Range)#//show clock.	

4.2.1.4 Help Function

There are two ways in SS2R24/48G4i switch Switch for the user to access help information the “help” command and the “?”.

Access to Help	Usage and function
Help	Under any command line prompt, type in “help” and press Enter will get a brief description of the associated help system.
“?”	1.Under any command line prompt, enter “?” to get a command list of the current mode and related brief description. 2.Enter a “?” after the command keyword with a embedded space. If the position should be a parameter, a description of that parameter type, scope, etc, will be returned; if the position should be a keyword, then a set of keywords with brief description will be returned; if the output is “<cr>“, then the command is complete, press Enter to run the command. 3.A “?” immediately following a string. This will display all the commands that begin with that string.

4.2.1.5 Input Verification

4.2.1.5.1 Returned Information success

All commands entered through keyboards undergo syntax check by the Shell. Nothing will be returned if the user entered a correct command under corresponding modes and the execution is successful.

4.2.1.5.2 Returned Information error

Returned Information error

Output error message	Explanation
Unrecognized command or illegal parameter!	The entered command does not exist, or there is error in parameter scope, type or format.
Ambiguous command	At least two interpretations is possible basing on the current input.
Invalid command or parameter	The command is recognized, but no valid parameter record is found.
This command is not exist in current mode	The command is recognized, but this command can not be used under current mode.
Please configure precursor command "*" at first !	The command is recognized, but the prerequisite command has not been configured.
syntax error missing "" before the end of command line!	Quotation marks are not used in pairs.

4.2.1.6 Fuzzy Match Support

SS2R24/48G4i switch switch shell support fuzzy match in searching command and keyword. Shell will recognize commands or keywords correctly if the entered string causes no conflict.

For example

1. For command “show interfaces status ethernet 1”, typing “sh in e 1” will work
2. However, for command “show running-config”, the system will report a “> Ambiguous command!” error if only “sh r” is entered, as Shell is unable to tell whether it is “show r” or “show running-config”. Therefore, Shell will only recognize the command if “sh ru” is entered.

4.2.2 Web Interfac

The Web configuration interface has three parts the upper part, the bottom left part and the bottom right part.

The upper part is a picture of the front panel of a SS2R24/48G4i switch switch, which can show the connection state of each port via the LEDs on the panel. If users click the port on the picture of the front panel, the statistic traffic information of each port will be displayed at the bottom right part of the Web

configuration interface.

The bottom left part of the Web configuration interface is the main menu, with which users can configure, control and maintain the switch, monitor ports and so on. The bottom right part is used to display information and to interact with users. When the users click the upper part or the bottom left part, the bottom right part will show the configuration interface of the corresponding menu(submenu), then, the users can configure the switch as they want to. To know more about the parameters appeared in the configuration interface, please refer to the configuration introduction in relative chapters.

Tips on using the Web Configuration Interface

Tip 1

IE6.0 or later/800*600 is recommened, and JavaScript is required to be enabled.

Tip 2

To guarantee the validity of the operation of CGI programs, the brower is required to read new stuff from the server every time instead of the system cache. The following steps will show you how to realize this Choose the Tools(T)->Internet Options from the menu of a Website or right click the IE browser on the desktop and choose Properities to enter the configuration interface. In the “Settings” dialog box of “Temporary Internet File”, under “Check for newer versions of stored pages”, click “Every visit to the page”.

Chapter 5 Basic Switch Configuration

5.1 Basic Switch Configuration Commands

Basic switch configuration includes commands for entering and exiting the admin mode, commands for entering and exiting interface mode, for configuring and displaying the switch clock, for displaying the version information of the switch system, etc.

Caution !!

By default, the host name of a switch and the command line prompt is the same as the type of the switch. In this chapter, “Switch” is used to represent general command line prompt.

5.1.1 clock set

Command clock set <*HH MM SS*> <*YYYY/MM/DD*>

Function to configure data and time setting

Parameter **<*HH MM SS* >**current time,***HH*** The number range 0~23, ***MM*** and ***SS The*** number range 0~59;**< *YYYY.MM.DD* >**current year/month/day, ***YYYY The*** number range 1970~2100, ***MM The*** number range 1~12, ***DD The*** number range 1~31.

Command mode privilege configuration mode

Default The default date is 2001—Jan-01 0 0 0.

Relative command **show clock**

5.1.2 config

Command **config [terminal]**

Function to convert from admin mode to global mode.

Parameter **[terminal]** to configure

Command mode Admin Mode

exec timeout

Command **exec timeout <*minutes* >**

Function to configure the overtime of quitting privileged configuration mode.

Parameter **< *minute* >**is time; the unit is minute(The range 0~300)

Command mode global mode

Default The default time is 5 minutes.

5.1.3 exit

Command exit

Function to quit from the current mode quit and return the previous mode. By this command, users being in global mode will return to admin configuration mode; users being admin mode will return to user mode.

Command mode All Modes

5.1.4 help

Command help

Function Output brief description of the command interpreter help system.

Command mode All Modes

5.1.5 ip host

Command ip host <hostname> <ip_addr>

no ip host <*hostname*>

Function Set the mapping relationship between the host and IP address; the “no ip host” parameter of this command will delete the mapping.

Parameter **<*hostname*>** is the host name, up to 15 characters are allowed; **<*ip_addr*>** is the corresponding IP address for the host name, takes a dot decimal format.

Command mode Global Mode

Relative command telnet、ping、traceroute

5.1.6 ip http server

Command ip http server

no ip http server

Function To enable the Web configuration; the “no no ip http server” command is used to disable the Web configuration.

Command Mode Global mode.

Relative Command web-user.

5.1.7 hostname

Command hostname <*hostname*>

Function Set the prompt in the switch command line interface.

Parameter <*hostname*> is the string for the prompt, up to 30 characters are allowed.

Command mode Global Mode

Default The default prompt is related to SS2R24/48G4i switch switch type.

5.1.8 reload

Command reload
Function Warm reset the switch.
Command mode Admin Mode
set default
Command set default
Function Reset the switch to factory settings.
Command mode Admin Mode

5.1.9 setup

Command setup
Function Enter the Setup Mode of the switch.
Command mode Admin Mode

5.1.10 language

Command language {chinese|english}
Function Set the language for displaying the help information.
Parameter Chinese for Chinese display; **English** for English display.
Command mode Admin Mode
Default The default setting is English display.

5.1.11 web-user

Command web-user <*username*> password {0|7} <*password*>
no web-user <*username*>
Function To set a username and its password for a Web client; the “no web-user <username>” command is used to delete this Web client.
Parameters <*username*>is an authorized username to do Web access, whose length should be no more than 16 characters; ***<password>*** is the access password, no longer than 8 characters; **0|7** respectively indicate to display the original or the encrypted password.
Command Mode Global configuration mode.
Relative Command ip http server

5.1.12 write

Command write
Function Save the currently configured parameters to the Flash memory.
Command mode Admin Mode

5.1.13 show cpu usage

Command show cpu usage
Function To display the CPU usage rate of the switch
Command Mode Admin Mode.
show tech-support
Command show tech-support
Function To collect tech-support information.
Command Mode Admin Mode.

5.2 Monitor and Debug Command

When the users configures the switch, they will need to verify whether the configurations are correct and the switch is operating as expected, and in network failure, the users will also need to diagnostic the problem. SS2R24/48G4i switch switch provides various debug commands including ping, telnet, show and debug, etc. to help the users to check system configuration, operating status and locate problem causes.

5.2.1 Ping

Command ping [<*ip-addr*>|<hostname>]
Function the switch sends ICMP request packet to remote client device and checks the communications between both sides is fine or not.
Parameter ***<ip-addr>***is destination host IP address, in dotted decimal notation.
<hostname> is destination host name, number and letter constitute character string.Blank is not allowed,the length of character string is from 1 to 30.
Default send 5 ICMP request packets; the packet size is 56 bytes; timeout is 2 seconds.
Command mode admin mode

5.2.2 Telnet

5.2.2.1 Introduction To Telnet

Telnet is a simple remote terminal protocol for remote login. Using Telnet, the user can login to a remote host with its IP address of hostname from his own workstation. Telnet can send the user's keystrokes to the remote host and send the remote host output to the user's screen through TCP connection. This is a transparent service, as to the user, the keyboard and monitor seems to be connected to the remote host directly.

Telnet employs the Client-Server mode, the local system is the Telnet client and the remote host is the Telnet server. SS2R24/48G4i switch switch can be either the Telnet Server or the Telnet client.

When SS2R24/48G4i switch switch is used as the Telnet server, the user can use the Telnet client program included in Windows or the other operation systems to login to SS2R24/48G4i switch switch,

as described earlier in the In-band management section. As a Telnet server, SS2R24/48G4i switch switch allows up to 5 telnet client TCP connections.

And as Telnet client, using **telnet** command under Admin Mode allows the user to login to the other remote hosts. SS2R24/48G4i switch switch can only establish TCP connection to one remote host. If a connection to another remote host is desired, the current TCP connection must be dropped.

5.2.2.2 Telnet Configuration Task List

1. Configuring Telnet Server

2. Telnet to a remote host from the switch

1. Configuration of Telnet Server

Command	Explanation
Global Mode	
telnet-server enable **no telnet-server enable**	Enable the Telnet server function in the switch the **"no telnet-server enable"** command disables the Telnet function.
telnet-user <*user-name*> password {0|7} <*password*> **no telnet-user <*user-name*>**	Configure the username and password to login to the switch through Telnet ,the **no telnet-user <*user-name*>** command disables Telnet accredited user.
telnet-server securityip <*ip-addr*> **no telnet-server securityip <*ip-addr*>**	Configure the secure IP address to login to the switch through Telnet the "**no telnet-server securityip <*ip-addr*>" command deletes the authorized Telnet secure address.**
authentication login {local|radius|local radius|radius local} **no authentication login**	Configure validatory mode of long-distance login in
Admin Mode	
Monitor **no monitor**	Display debug information for Telnet client login to the switch; the "**no monitor"** command disables the debug information.

2. Telnet to a remote host from the switch

Command	Explanation
Admin Mode	
telnet [<*ip-addr*>] [<*port*>]	Login to a remote host with the Telnet client included in the switch.

5.2.2.3 Commands for Telnet

5.2.2.3.1 authentication login

Command authentication login {local | radius | local radius | radius local}

no authentication login

Function To configure the Telnet Server to set the password authentication mode and privilege of remote access users; the “no authentication login” command is used to reset it to the default authentication mode.

Default Setting The default access authentication mode is local.

Command Mode Global mode.

Relative Command aaa enable，radius-server authentication host

5.2.2.3.2 monitor

Command monitor

no monitor

Function to make Telnet clients display debug information, and disable Console clients to display debug information function. Use the “no’ command to disable Telnet client display debug information function and restore Console client display debug information function.

Command mode Admin mode

Relative Command telnet-user

5.2.2.3.3 telnet

Command telnet [<*ip-addr*>|<*ip-host-name*>] [<*port*>]

Parameter ***<ip-addr>*** is the IP address of the remote host,shown in dotted decimal notation;***<hostname>*** is the name of the remote host,containing max 30 characters;***<port>*** is the port number,ranging between 0~65535.

Command Mode Admin Mode

Relative Command ip host

5.2.2.3.4 telnet-server enable

Command telnet-server enable

no telnet-server enable

Function Enable the Telnet server function in the switch the “**no telnet-server enable”** command

disables the Telnet function in the switch.

Default Telnet server function is enabled by default.

Command mode Global Mode

5.2.2.3.5 telnet-server securityip

Command **telnet-server securityip <*ip-addr*>**

no telnet-server securityip <*ip-addr*>

Function Configure the secure IP address of Telnet client allowed to login to the switch; the "**no telnet-server securityip <*ip-addr*>"** command deletes the authorized Telnet secure address.

Parameter ***<ip-addr>*** is the secure IP address allowed to access the switch, in dot decimal format.

Default no secure IP address is set by default.

Command mode Global Mode

5.2.2.3.6 telnet-user

Command telnet-user <*username*> password {0|7} <*password*>

no telnet-user <*username*>

Function to configure user names and passwords of Telnet clients. Use the "**no telnet-user <*username*>**" command to remove the Telnet users.

Parameter ***<username>is the*** Telnet client user name. The maximum length may not exceed 16 characters; ***<password>is the*** login password, the maximum length may not exceed 8 characters; **0|7** part means as passwords displayed not encrypted or encrypted

Command mode global configuration mode

Default The default system does not configure Telnet client user name and password.

5.2.3 SSH

5.2.3.1 Introduction to SSH

SSH (Secure Shell) is a protocol which ensures a secure remote access connection to network devices. It is based on the reliable TCP/IP protocol. By conducting the mechanism such as key distribution, authentication and encryption between SSH server and SSH client, a secure connection is established. The information transferred on this connection is protected from being intercepted and decrypted. The switch meets the requirements of SSH2.0. It supports SSH2.0 client software such as SSH Secure Client and putty. Users can run the above software to manage the switch remotely.

The switch presently supports RSA authentication, 3DES cryptography protocol and SSH user password authentication etc.

5.2.3.2 SSH Server Configuration Task List

1. SSH Server Configuration

Command	Explanation
Global Mode	
ssh-server enable **no ssh-server enable**	Enable SSH function on the switch; the "**no ssh-server enable**" command disables SSH function.
ssh-user <*user-name*> password {0|7} <*password*> **no ssh-user <*user-name*>**	Configure the username and password of SSH client software for logging on the switch; the "**no ssh-user <user-name>**" command deletes the username.
ssh-server timeout <*timeout*> **no ssh-server timeout**	Configure timeout value for SSH authentication; the "**no ssh-server timeout**" command restores the default timeout value for SSH authentication.
ssh-server authentication-retires <*authentication-retires*> **no ssh-server authentication-retries**	Configure the number of times for retrying SSH authentication; the "**no ssh-server authentication-retries**" command restores the default number of times for retrying SSH authentication.
ssh-server host-key create rsa modulus <*moduls*>	Generate the new RSA host key on the SSH server.
Admin Mode	
monitor **no monitor**	Display SSH debug information on the SSH client side; the "**no monitor**" command stops displaying SSH debug information on the SSH client side.

5.2.3.3 Commands for SSH

5.2.3.3.1 ssh-server enable

Command ssh-server enable
no ssh-server enable
Function Enable SSH function on the switch; the "**no ssh-server enable**" command disables SSH function.
Command mode **Global Mode**
Default SSH function is disabled by default.

5.2.3.3.2 ssh-user

Command **ssh-user <*username*> password {0|7} <*password*>**
no ssh-user <*username*>

Function Configure the username and password of SSH client software for logging on the switch; the "**no ssh-user <user-name>**" command deletes the username.

Parameter ***<username>*** is SSH client username. It can't exceed 16 characters; ***<password>*** is SSH client password. It can't exceed 8 characters; **0|7** stand for unencrypted password and encrypted password.

Command mode **Global Mode**

Default There are no SSH username and password by default.

5.2.3.3.3 ssh-server timeout

Command **ssh-server timeout <*timeout*>**

no ssh-server timeout

Function Configure timeout value for SSH authentication; the "**no ssh-server timeout**" command restores the default timeout value for SSH authentication.

Parameter ***<timeout>*** is timeout value; valid range is 10 to 600 seconds.

Command mode **Global Mode**

Default SSH authentication timeout is 180 seconds by default.

5.2.3.3.4 ssh-server authentication-retries

Command ssh-server authentication-retries < authentication-retries >

no ssh-server authentication-retries

Function Configure the number of times for retrying SSH authentication; the "**no ssh-server authentication-retries**" command restores the default number of times for retrying SSH authentication.

Parameter **< authentication-retries >** is the number of times for retrying authentication; valid range is 1 to 10.

Command mode **Global Mode**

Default The number of times for retrying SSH authentication is 3 by default.

5.2.3.3.5 ssh-server host-key create rsa

Command ssh-server host-key create rsa [modulus < modulus >]

Function Generate new RSA host key

Parameter **modulus** is the modulus which is used to compute the host key; valid range is 768 to 2048. The default value is 1024.

Command mode **Global Mode**

Default The system uses the key generated when the ssh-server is started at the first time.

5.2.3.3.6 monitor

Command monitor

no monitor

Function Display SSH debug information on the SSH client side; at the same time disable function of debug information in console,the "**no monitor**" command stops displaying SSH debug information on

the SSH client side,enable function of debug information in console

Command mode **Admin Mode**

Relative Command **ssh-user**

5.2.3.4 SSH Server Configure Example

Scenario 1

Requirement Enable SSH server on the switch, and run SSH2.0 client software such as Secure shell client and putty on the terminal. Log on the switch by using the username and password from the client.

Configure the IP address, add SSH user and enable SSH service on the switch. SSH2.0 client can log on the switch by using the username and password to configure the switch.

```
Switch(Config)#interface vlan 1
Switch(Config-Vlan-1)#ip address 100.100.100.200 255.255.255.0
Switch(Config-Vlan-1)#exit
Switch(Config)#ssh-user test password 0 test
Switch(Config)#ssh-server enable
```

5.2.3.5 SSH Monitor and Debug Command

5.2.3.5.1 show ssh-user

Command show ssh-user

Function To display all the configured SSH usernames.

Command Mode Admin Mode.

Relative Command ssh-user

5.2.3.5.2 show ssh-server

Command show ssh-server

Function To display the state of SSH server(open or closed) and the information of users who has already logged in.

Command Mode Admin Mode.

Relative Command ssh-server enable，no ssh-server enable

5.2.3.5.3 debug ssh-server

Command debug ssh-server

no debug ssh-server

Function To enable the debug information of SSH server. The “no debug ssh-server ” command is used to disable the debug information of SSH server.

Default Setting By default, the debug information is disabled.

Command Mode Admin Mode.

5.2.4 Traceroute

Command traceroute {*<ip-addr>* | host *<hostname>* }[hops *<hops>*] [timeout *<timeout>*]
Function This command is used to test the gateways passed by packets on their way from sending equipment to destination equipment, in order to check whether the network can be reached and to locate the fault of network.
Parameters ***<ip-addr>***is the IP address of the destination host, in dotted-decimal format; ***<hostname>***is the host name of the remote host. ***<hops>*** is the max number of passed gateways allowed by Traceroute. ***<timeout>***is the timeout value of packets, in millisecond, ranging from 100 to 10000.
Default Setting The max number of passed gateways is set by default as 16, while the timeout value is 2000 milliseconds.
Command Mode Admin Mode.
Relative Command ip host

5.2.5 Show

show command is used to display information about the system , port and protocol operation. This part introduces the **show** command that displays system information, other **show** commands will be discussed in other chapters.

5.2.5.1 show arp

Command show arp
Function Display ARP Mapping table
Command Mode Admin Mode

5.2.5.2 show clock

Command show clock
Function Display current system clock
Command Mode Admin Mode
Relative Command clock set

5.2.5.3 show debugging

Command show debugging
Function Display the debugging state
Command Mode Admin Mode
Relative Command debug

5.2.5.4 show flash

Command show flash
Function Display the document in the flash
Command Mode Admin Mode

5.2.5.5 show history

Command show history
Function Display the recent user input history command
Command Mode Admin Mode

5.2.5.6 show memory

Command show memory
Function Display the contents in the memory
Command Mode Admin Mode

5.2.5.7 show rom

Command show rom
Function Display enable document and bulk
Command Mode Admin Mode

5.2.5.8 show running-config

Command show running-config
Function Display the current active configuration parameters for the switch.
Default If the active configuration parameters are the same as the default operating parameters, nothing will be displayed.
Command mode Admin Mode

5.2.5.9 show startup-config

Command show startup-config
Function Display the switch parameter configurations written into the Flash memory at the current operation; those are usually also the configuration files used for the next power-up.
Default If the configuration parameters read from the Flash are the same as the default operating parameter, nothing will be displayed.
Command mode Admin Mode

5.2.5.10 show switchport interface

Command show switchport interface [ethernet <interface-list>]
Function Show the VLAN port mode, VLAN number and Trunk port messages of the VLAN port mode on the switch.
Parameter ***<interface-list>*** is the port number or port list, which could be maximum of 0/0/1 port in

the switch

5.2.5.11 show tcp

Command show tcp
Function Display the current TCP connection status established to the switch.
Command mode Admin Mode

5.2.5.12 show udp

Command show udp
Function Display the current UDP connection status established to the switch.
Command mode Admin Mode

5.2.5.13 show telnet login

Command show telnet login
Function Display Telnet user information that links with the switch

5.2.5.14 show telnet user

Command show telnet user
Function Display all Telnet user information that can login the switch via Telnet.
Relative Command telnet-user password

5.2.5.15 show version

Command show version
Function Display the switch version.
Command mode Admin Mode

5.2.6 Debug

All the protocols SS2R24/48G4i switch switch supports have their corresponding debug commands. The users can use the information from debug commands for troubleshooting. Debug commands for their corresponding protocols will be introduced in the later chapters.

5.3 Configure the IP Address of the Switch

In theory, SS2R24/48G4i switch switch is a layer 2(Data Link Layer)device, which should not have an IP address, because IP address is a concept belonged to layer 3(Network Layer).But, as a device used in network, switch needs a network address to be its unique identifier, so that the network manager can identify and control it.

The IP address of SS2R24/48G4i switch switch is set on the VLAN interface. The VLAN with an IP address is called management VLAN. All the in-band management of the switch is done through management VLAN.SS2R24/48G4i switch switch only allows one VLAN interface, so, to change the ID of the management VLAN, the original VLAN interface should be deleted first, and then create a new VLAN interface.

SS2R24/48G4i switch switch provides three IP address configuration methods

- Manual
- BootP
- DHCP

Manual configuration of IP address is assign an IP address manually for the switch.

In BootP/DHCP mode, the switch operates as a BootP/DHCP client, send broadcast packets of BootPRequest to the BootP/DHCP servers, and the BootP/DHCP servers assign the address on receiving the request. In addition, SS2R24/48G4i switch switch can act as a DHCP server, and dynamically assign network parameters such as IP addresses, gateway addresses and DNS server addresses to DHCP clients DHCP Server configuration is detailed in later chapters.

Switch IP Addresses Configuration Task List

1. Manual configuration
2. BootP configuration
3. DHCP configuration

1. Manual configuration

Command	Explanation
ip address <*ip_address*> <*mask*> **no ip address <*ip_address*> <*mask*>**	Configure IP address of the switch; the "**no ip address <*ip_address*> <*mask*>**" command deletes IP address of the switch.

2. BootP configuration

Command	Explanation
ip bootp-client enable **no ip bootp-client enable**	Enable the switch to be a BootP client and obtain IP address and gateway address through BootP negotiation; the **no ip bootp-client enable**" command disables the BootP client function.

3.DHCP

Command	Explanation
ip dhcp-client enable **no ip dhcp-client enable**	Enable the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the "**no ip dhcp-client enable**" command disables the DHCP client function.

5.4 SNMP Configuration

5.4.1 Introduction To SNMP

SNMP (Simple Network Management Protocol) is a standard network management protocol widely used in computer network management. SNMP is an evolving protocol. SNMP v1 [RFC1157] is the first version of SNMP which is adapted by vast numbers of manufacturers for its simplicity and easy implementation; SNMP v2c is an enhanced version of SNMP v1, which supports layered network management; SNMP v3 strengthens the security by adding USM (User-based Security Mode) and VACM (View-based Access Control Model).

SNMP protocol provides a simple way of exchange network management information between two points in the network. SNMP employs a polling mechanism of message query, and transmits messages through UDP (a connectionless transport layer protocol). Therefore it is well supported by the existing computer networks.

SNMP protocol employs a station-agent mode. There are two parts in this structure NMS (Network Management Station) and Agent. NMS is the workstation on which SNMP client program is running. It is the core on the SNMP network management. Agent is the server software runs on the devices which need to be managed. NMS manages all the managed objects through Agents. The switch supports Agent function.

The communication between NMS and Agent functions in Client/Server mode by exchanging standard messages. NMS sends request and the Agent responds. There are seven types of SNMP message

- Get-Request
- Get-Response
- Get-Next-Request
- Get-Bulk-Request
- Set-Request
- Trap
- Inform-Request

NMS sends queries to the Agent with Get-Request, Get-Next-Request, Get-Bulk-Request and Set-Request messages; and the Agent, upon receiving the requests, replies with Get-Response message. On some special situations, like network device ports are on Up/Down status or the network topology changes, Agents can send Trap messages to NMS to inform the abnormal events. Besides, NMS can also be set to alert to some abnormal events by enabling RMON function. When alert events are triggered, Agents will send Trap messages or log the event according to the settings. Inform-Request is mainly used for inter-NMS communication in the layered network management.

USM ensures the transfer security by well-designed encryption and authentication. USM encrypts the messages according to the user typed password. This mechanism ensures that the messages can’t be viewed on transmission. And USM authentication ensures that the messages can’t be changed on transmission. USM employs DES-CBC cryptography. And HMAC-MD5 and HMAC-SHA are used for authentication.

VACM is used to classify the users’ access permission. It puts the users with the same access permission in the same group. Users can’t conduct the operation which is not authorized.

5.4.2 Introduction to MIB

The network management information accessed by NMS is well defined and organized in a Management Information Base (MIB). MIB is pre-defined information which can be accessed by network management protocols. It is in layered and structured form. The pre-defined management information can be obtained from monitored network devices. ISO ASN.1 defines a tree structure for MID. Each MIB organizes all the available information with this tree structure. And each node on this tree contains an OID (Object Identifier) and a brief description about the node. OID is a set of integers divided by periods. It identifies the node and can be used to locate the node in a MID tree structure, shown in the figure below

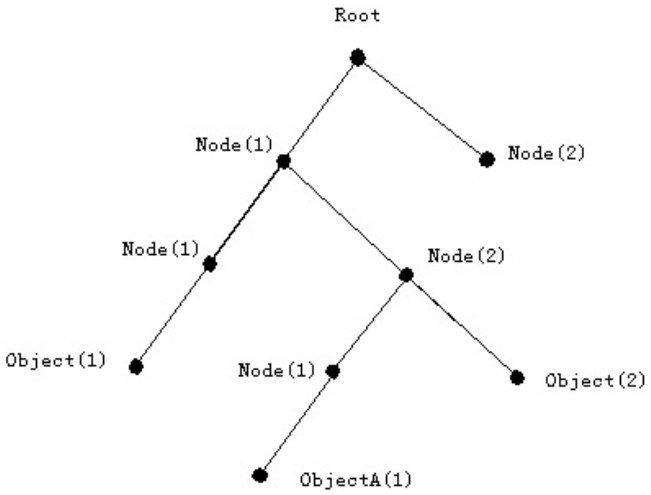


Fig 5-1 ASN.1 Tree Instance

In this figure, the OID of the object A is 1.2.1.1. NMS can locate this object through this unique OID and gets the standard variables of the object. MIB defines a set of standard variables for monitored network devices by following this structure.

If the variable information of Agent MIB needs to be browsed, the MIB browse software needs to be run on the NMS. MIB in the Agent usually consists of public MIB and private MIB. The public MIB contains public network management information that can be accessed by all NMS; private MIB contains specific information which can be viewed and controlled by the support of the manufacturers

MIB-I [RFC1156] is the first implemented public MIB of SNMP, and is replaced by MIB-II [RFC1213]. MIB-II expands MIB-I and keeps the OID of MIB tree in MIB-I. MIB-II contains sub-trees which are called groups. Objects in those groups cover all the functional domains in network management. NMS obtains the network management information by visiting the MIB of SNMP Agent.

The switch can operate as a SNMP Agent, and supports both SNMP v1/v2c and SNMP v3. The switch supports basic MIB-II, RMON public MIB and other public MID such as BRIDGE MIB. Besides, the switch supports self-defined private MIB.

5.4.3 Introduction to RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9

Statistics Maintain basic usage and error statistics for each subnet monitored by the Agent.

History Record periodical statistic samples available from Statistics.

Alarm Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.

Event A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

5.4.4 SNMP Configuration

5.4.4.1 SNMP Configuration Task List

1. Enable or disable SNMP Agent server function
2. Configure SNMP community string
3. Configure IP address of SNMP management base
4. Configure engine ID
5. Configure user
6. Configure group
7. Configure view
8. Configuring TRAP
9. Enable/Disable RMON

1. Enable or disable SNMP Agent server function

Command	Explanation
snmp-server enable no snmp-server enable	Enable the SNMP Agent function on the switch; the “no snmp-server enable” command disables the SNMP Agent function on the switch.

2. Configure SNMP community string

Command	Explanation
snmp-server community {ro|rw} <*string*> no snmp-server community <*string*>	Configure the community string for the switch; the "no snmp-server community <*string*>" command deletes the configured community string.

3. Configure IP address of SNMP management base

Command	Explanation
snmp-server securityip <*ip-address*> no snmp-server securityip <*ip-address*>	Configure the secure IPv4/IPv6 address which is allowed to access the switch on the NMS; the "no snmp-server securityip <*ip-address*> " command deletes configured secure address.
snmp-server SecurityIP enable snmp-server SecurityIP disable	Enable or disable secure IP address check function on the NMS.

4. Configure engine ID

Command	Explanation
snmp-server engineid < *engine-string* > no snmp-server engineid < *engine-string* >	Configure the local engine ID on the switch. This command is used for SNMP v3.

5. Configure user

Command	Explanation
snmp-server user <*user-string*> <*group-string*> [[encrypted] {auth {md5|sha} <*password-string*>}] no snmp-server user <*user-string*> <*group-string*>	Add a user to a SNMP group. This command is used to configure USM for SNMP v3.

6.Configure group

Command	Explanation
snmp-server group <*group-string*> {NoauthNopriv|AuthNopriv|AuthPriv} [[read <*read-string*>] [write <*write-string*>] [notify <*notify-string*>]] no snmp-server group <*group-string*> {NoauthNopriv|AuthNopriv|AuthPriv}	Set the group information on the switch. This command is used to configure VACM for SNMP v3.

7. Configure view

Command	Explanation
snmp-server view <*view-string*> <*oid-string*> {include|exclude} no snmp-server view <*view-string*>	Configure view on the switch. This command is used for SNMP v3.

8. Configuring TRAP

Command	Explanation
snmp-server enable traps no snmp-server enable traps	Enable the switch to send Trap message. This command is used for SNMP v1/v2/v3.
snmp-server host <*host-address* > {v1|v2c|{v3 {NoauthNopriv|AuthNopriv|AuthPriv}}} <*user-string*> no snmp-server host <*host-address*> {v1|v2c|{v3 {NoauthNopriv|AuthNopriv|AuthPriv}}} <*user-string*>	Set the host IPv4/IPv6 address which is used to receive SNMP Trap information. For SNMP v1/v2, this command also configures Trap community string; for SNMP v3, this command also configures Trap user name and security level.

9. Enable/Disable RMON

Command	Explanation
rmon enable no rmon enable	Enable/disable RMON.

5.4.5 Typical SNMP Configuration Examples

The IP address of the NMS is 1.1.1.5; the IP address of the switch (Agent) is 1.1.1.9

Scenario 1 The NMS network administrative software uses SNMP protocol to obtain data from the switch.

The configuration on the switch is listed below

Switch(config)#snmp-server enable
Switch(Config)#snmp-server community rw private
Switch(Config)#snmp-server community ro public
Switch(Config)#snmp-server securityip 1.1.1.5

The NMS can use “private” as the community string to access the switch with read-write permission, or use “public” as the community string to access the switch with read-only permission.

Scenario 2 NMS will receive Trap messages from the switch (Note NMS may have community string verification for the Trap messages. In this scenario, the NMS uses a Trap verification community string of “dcntrap”).

The configuration on the switch is listed below
Switch(config)#snmp-server enable
Switch(Config)#snmp-server host 1.1.1.5 v1 dcntrap
Switch(Config)#snmp-server enable traps

Scenario 3 NMS uses SNMP v3 to obtain information from the switch.

The configuration on the switch is listed below
Switch(config)#snmp-server enable

Switch (Config)#snmp-server user tester DCNGroup encrypted auth md5 hello
Switch (Config)#snmp-server group DCNGroup AuthPriv read max write max notify max
Switch (Config)#snmp-server view max 1 include

Scenario 4 NMS wants to receive the v3Trap messages sent by the switch.
The configuration on the switch is listed below
Switch(config)#snmp-server enable
Switch(config)#snmp-server host 10.1.1.2 v3 AuthPriv tester
Switch(config)#snmp-server enable traps

5.4.6 SNMP Troubleshooting

5.4.6.1 Monitor and Debug Command

5.4.6.1.1 show snmp

Command **show snmp**
Function Display all SNMP counter information.
Command mode Admin Mode

Displayed information	Explanation
snmp packets input	Total number of SNMP packet inputs.
bad snmp version errors	Number of version information error packets.
unknown community name	Number of community name error packets.
illegal operation for community name supplied	Number of permission for community name error packets.
encoding errors	Number of encoding error packets.
number of requested variablest	Number of variables requested by NMS.
number of altered variables	Number of variables set by NMS.
get-request PDUs	Number of packets received by “get” requests.
get-next PDUs	Number of packets received by “getnext” requests.
set-request PDUs	Number of packets received by “set” requests.
snmp packets output	Total number of SNMP packet outputs.
too big errors	Number of “Too_ big” error SNMP packets.

maximum packet size	Maximum length of SNMP packets.
no such name errors	Number of packets requesting for non-existent MIB objects.
bad values errors	Number of “Bad_values” error SNMP packets.
general errors	Number of “General_errors” error SNMP packets.
response PDUs	Number of response packets sent.
trap PDUs	Number of Trap packets sent.

5.4.6.1.2 show snmp status

Command show snmp status
Function Display SNMP configuration information.
Command mode Admin Mode

Displayed information	Description
System Name	Switch name
System Contact	Contact mode
System Location	Switch Location
Trap disable	Disable Trap Function
RMON enable	Enable RMON Function
Community Information	Community Information
Security IP is Enabled	Enabled Security IP Function
V1/V2c Trap Host Information	Receive V1/V2c Trap Host Information
V3 Trap Host Information	Receive V3 Trap Host Information

5.4.6.1.3 show snmp engineid

Command show snmp engineid
Function Display the engine ID commands
Command Mode Admin Mode

Displayed Information	Explanation
SNMP engineID	Engine number
Engine Boots	Engine boot counts

5.4.6.1.4 show snmp user

Command show snmp user
Function Display the user information commands
Command Mode Admin Mode

Displayed Information	Explanation
User name	User name
Engine ID	Engine ID
Priv Protocol	Employed encryption algorithm
Auth Protocol	Employed identification algorithm
Row status	User state

5.4.6.1.5 show snmp group

Command show snmp group
Function Display the group information commands
Command Mode Admin Mode

Displayed Information	Explanation
Group Name	Group name
Security level	Security level
Read View	Read view name
Write View	Write view name
Notify View	Notify view name
<no writeview specified>	No view name specified by the user

5.4.6.1.6 show snmp view

Command show snmp view
Function Display the view information commands.
Command Mode Admin Mode

Displayed Information	Explanation
View Name	View name
1.and1.3.	OID number
Included	The view includes sub trees rooted by this OID
Excluded	The view does not include sub trees rooted by this OID
active	State

5.4.6.1.7 show snmp mib

Command show snmp mib
Function Display all MIB supported by the switch
Command Mode Admin Mode

5.4.6.1.8 debug snmp packet

Command debug snmp packet
no debug snmp packet
Function Enable the SNMP debugging; the "**no debug snmp packet**" command disables the debugging function
Command Mode Admin Mode

5.4.6.2 SNMP Troubleshooting

When users configure the SNMP, the SNMP server may fail to run properly due to physical connection failure and wrong configuration, etc. Users can troubleshoot the problems by following the guide below

- Good condition of the physical connection.
- Interface and datalink layer protocol is Up (use the "show interface" command), and the connection between the switch and host can be verified by ping (use "ping" command).
- The switch enabled SNMP Agent server function (use "snmp-server" command)
- Secure IP for NMS (use "snmp-server securityip" command) and community string (use "snmp-server community" command) are correctly configured, as any of them fails, SNMP will not be able to communicate with NMS properly.
- If Trap function is required, remember to enable Trap (use "snmp-server enable traps" command). and remember to properly configure the target host IP address and community string for Trap (use "snmp-server host" command) to ensure Trap message can be sent to the specified host.
- If RMON function is required, RMON must be enabled first (use "rmon enable" command).
- Use "show snmp" command to verify sent and received SNMP messages; Use "show snmp status" command to verify SNMP configuration information; Use "debug snmp packet" to enable SNMP debug function and verify debug information.
- If users still can't solve the SNMP problems, Please contact our technical and service center.

5.5 Switch Upgrade

SS2R24/48G4i switch switch provides two ways for switch upgrade BootROM upgrade and the TFTP/FTP upgrade under Shell

5.5.1 BootROM Upgrade

There are two methods for BootROM upgrade TFTP and FTP, which can be selected at BootROM command settings.
The upgrade procedures are listed below
Step 1
A PC is used as the console for the switch. A console cable is used to connect PC to the management port on the switch. The PC should have FTP/TFTP server software installed and has the img file required for the upgrade.
Step 2
Press “ctrl+b” on switch boot up until the switch enters BootROM monitor mode. The operation result is shown below

```
Testing RAM...
0x00200000 RAM OK

Loading BootRom...
Starting BootRom.....

CPU    88E6218 133MHZ
BSP version    1.2.21
Creation date    Mar 12 2007, 10 27 58

Initializing... OK!

[Boot]
```

Step 3
Under BootROM mode, run “setconfig” to set the IP address and mask of the switch under BootROM mode, server IP address and mask, and select TFTP or FTP upgrade. Suppose the switch address is 192.168.1.2/24, and PC address is 192.168.1.66/24, and select TFTP upgrade, the configuration should like

```
[Boot]    setconfig
Host IP Address    10.1.1.1    192.168.1.189
Server IP Address    10.1.1.2    192.168.1.101
FTP(1) or TFTP(2)    1    2
Network interface configure OK.
[Boot]
```

Step 4
Enable FTP/TFTP server in the PC. For TFTP, run TFTP server program; for FTP, run FTP server program. Before start downloading upgrade file to the switch, verify the connectivity between the server and the switch by ping from the server. If ping succeeds, run “load” command in the BootROM mode from the switch; if it fails, perform troubleshooting to find out the cause. The following is the configuration for the system update image file.

Loading...
entry = 0x10010
size = 0x1077f8

Step 5
Execute “write nos.img” in BootROM mode. The following saves the system update image file.

[Boot] writeimg
Programming...

Program OK.

Step 6
After successful upgrade, execute “run” command in BootROM mode to return to CLI configuration interface.

5.5.2 FTP/TFTP Upgrade

5.5.2.1 Introduction To FTP/TFTP

FTP(File Transfer Protocol)/TFTP(Trivial File Transfer Protocol) are both file transfer protocols that belonging to fourth layer(application layer) of the TCP/IP protocol stack, used for transferring files between hosts, hosts and switches. Both of them transfer files in a client-server model. Their differences are listed below.

FTP builds upon TCP to provide reliable connection-oriented data stream transfer service. However, it does not provide file access authorization and uses simple authentication mechanism(transfers username and password in plain text for authentication). When using FTP to transfer files, two connections need to be established between the client and the server a management connection and a data connection. A transfer request should be sent by the FTP client to establish management connection on port 21 in the server, and negotiate a data connection through the management connection.

There are two types of data connections active connection and passive connection.

In active connection, the client transmits its address and port number for data transmission to the sever, the management connection maintains until data transfer is complete. Then, using the address and port number provided by the client, the server establishes data connection on port 20 (if not engaged) to transfer data; if port 20 is engaged, the server automatically generates some other port number to establish data connection.

In passive connection, the client, through management connection, notify the server to establish a passive connection. The server then creates its own data listening port and informs the client about the port, and the client establishes data connection to the specified port.

As data connection is established through the specified address and port, there is a third party to provide data connection service.

TFTP builds upon UDP, providing unreliable data stream transfer service with no user

authentication or permission-based file access authorization. It ensures correct data transmission by sending and acknowledging mechanism and retransmission of time-out packets. The advantage of TFTP over FTP is that it is a simple and low overhead file transfer service.

SS2R24/48G4i switch switch can operate as either FTP/TFTP client or server. When SS2R24/48G4i switch switch operates as a FTP/TFTP client, configuration files or system files can be downloaded from the remote FTP/TFTP servers(can be hosts or other switches) without affecting its normal operation. And file list can also be retrieved from the server in ftp client mode. Of course, SS2R24/48G4i switch switch can also upload current configuration files or system files to the remote FTP/TFTP servers(can be hosts or other switches). When SS2R24/48G4i switch switch operates as a FTP/TFTP server, it can provide file upload and download service for authorized FTP/TFTP clients, as file list service as FTP server.

Here are some terms frequently used in FTP/TFTP.

ROM Short for EPROM, erasable read-only memory. EPROM is repalced by FLASH memory in SS2R24/48G4i switch switch.

SDRAM RAM memory in the switch, used for system software operation and configuration sequence storage.

FLASH Flash memory used to save system file and configuration file

System file including system image file and boot file.

System image file refers to the compressed file for switch hardware driver and software support program, usually refer to as IMAGE upgrade file. In SS2R24/48G4i switch switch, the system image file is allowed to save in FLASH only. SS2R24/48G4i switch switch mandates the name of system image file to be uploaded via FTP in Global Mode to be nos.img, other IMAGE system files will be rejected.

Boot file refers to the file initializes the switch, also referred to as the ROM upgrade file (Large size file can be compressed as IMAGE file). In SS2R24/48G4i switch switch, the boot file is allowed to save in ROM only. SS2R24/48G4i switch switch mandates the name of the boot file to be boot.rom.

Configuration file including start up configuration file and running configuration file. The distinction between start up configuration file and running configuration file can facilitate the backup and update of the configurations.

Start up configuration file refers to the configuration sequence used in switch start up. SS2R24/48G4i switch switch start up configuration file stores in FLASH only, corresponding to the so called configuration save. To prevent illicit file upload and easier configuration, SS2R24/48G4i switch switch mandates the name of start up configuration file to be startup-config.

Running configuration file refers to the running configuration sequence use in the switch. In SS2R24/48G4i switch switch, the running configuration file stores in the RAM. In the current version, the running configuration sequence running-config can be saved from the RAM to FLASH by **write** command or **copy running-config startup-config** command, so that the running configuration sequence becomes the start up configuration file, which is called configuration save. To prevent illicit file upload and easier configuration, SS2R24/48G4i switch switch mandates the name of running configuration file to be running-config.

Factory configuration file The configuration file shipped with SS2R24/48G4i switch switch in the name of factory-config. Run **set default** and **write**, and restart the switch, factory configuration file will be loaded to overwrite current start up configuration file.

5.5.2.2 FTP/TFTP Configuration

The configurations of SS2R24/48G4i switch switch as FTP and TFTP clients are almost the same, so the configuration procedures for FTP and TFTP are described together in this manual.

5.5.2.2.1 FTP/TFTP Configuration Task List

1. FTP/TFTP client configuration

Upload/download the configuration file or system file.

（1） For FTP client, server file list can be checked.

2. FTP server configuration

（1）Start FTP server

（2）Configure FTP login username and password

（3）Modify FTP server connection idle time

（4）Shut down FTP server

3. TFTP server configuration

（1）Start TFTP server

（2）Configure TFTP server connection idle time

（3）Configure retransmission times before timeout for packets without acknowledgement

（4）Shut down TFTP server

1. FTP/TFTPconfiguration

(1)FTP client upload/download file

Command	**Explanation**
Admin Mode	
copy <*source-url*> <*destination-url*> [ascii | binary]	FTP/TFTP client upload/download file
Global Mode	
Dir <ftpServerUrl>	For FTP client, server file list can be checked. *FtpServerUrl* format looks like ftp //user password@IP Address

2.FTP server configuration

(1)Start FTP server

Command	**Explanation**
Global Mode	
ftp-server enable **no ftp-server enable**	Start FTP server, the “**no ftp-server enable**” command shuts down FTP server and prevents FTP user from logging in.

(2)Set usename and password for FTP logging in

Command	Explanation
Global Mode	
ip ftp-server username <*username*> password {0|7} <*password*> **no ip ftp-server username <*username*>**	Set FTP server ‘s username and password when logging in.

(3)Modify FTP server connection idle time

Command	**Explanation**
Global Mode	
ftp-server timeout <seconds> **no ftp-server timeout**	set connection idle time。

3.TFTP server configuration(1)Start TFTP server

Command	**Explanation**
Global Mode	
tftp-server enable **no tftp-server enable**	Start TFTP server, the "**no ftp-server enable**" command shuts down TFTP server and prevents TFTP user from logging in.

(2)Modify TFTP server connection idle time

Command	**Explanation**
Global Mode	
tftp-server transmission-timeout <seconds>	Set maximum retransmission time within timeout interval.

(3)Modify TFTP server connection retransmission time

Command	**Explanation**
Global Mode	
tftp-server retransmission-number <*number*>	Set maximum retransmission time within timeout interval.

5.6 The three-level switch of log message

5.6.1 Introduction to the system log

System log takes control of the output of most information and is able to effectively filter the information because of its ability to do fine-grain classification. Its combination with Debug program provides a powerful support for the network managers and developers to monitor the operation of network and diagnose the problems of network.

The system log features include

- Support the system log output in four directions Console, Telnet terminal and Dumb terminal(monitor), logbuf, and loghost.
- The log information can be divided into four levels according to different importance, and thus can be filtered by level.
- The log information can be divided according to different source modules, and thus can be filtered by module.

5.6.1.1 Log Output Channel

At present, the system log of the switch can be outputted through five directions(aka log channels)

- Output log information to local console through Console port.
- Output log information to remote Telnet terminal or Dumb terminal, which helps remote maintenance.
- Allocate log buffer of proper size inside the switch to record log information.
- Configure loghost. The log system will directly send log information to loghost, and save it in the form of file in the loghost so the information can be reviewed on demand.

5.6.1.2 Format And Severity Of The Log Information

The log information format is compatible with the 4.3 BSD UNIX syslog protocol, so we can record and analyze the log by the systlog (system log protect session) on the UNIX/LINUX, as well as syslog similar applications on PC.

The log information is classified into eight classes by severity or emergency procedure. One level per value and the higher the emergency level the log information has, the smaller its value will be. For example, the level of critical is 2, and warning is 4, debugging is leveled at 7, so the critical is higher than warnings which no doubt is high than debugging.

Severity	Value	Description	Syslog define
critical	2	Critical conditions	LOG_CRIT
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
debugging	7	Debugging messages	LOG_DEBUG

Right now the switch can generate information of following two levels

- Up/down switch, topology change, aggregate port state change of the interface are classified warnings
- The display level of the output monitored by shell Configure command is notifications.

Attention By default the system log is disabled. When it is enabled, because of the classification and output of the information, especially when there is a large amount of information under processing, the system performance will be effected.

5.6.1.3 The three-level switch of log message

The system log uses a three-level switch architecture to control the output of the log message global log switch, log output channel state and the module state of channel filter Items.

- Only when the global switch is on, the log message are written to the log message queue.
- After the switch boots, the system log task is started. The aim of this task is to read out every log message from the log message queue, and to send them out through every output channel. Only when the output channel is in “Enable” state, the log message can be sent out through it.

When the log message enters the output channel, it will be checked according to the output channel’s filter items, only when the source module of the log message is marked as “On” in the filter items, the

log message can be actually sent out through the output channel.

5.6.2 Configuring The System Log

5.6.2.1 The Task Sequence of Configuring The System Log

1. Set the global log switch
2. Set the output channel of the console.
3. Set the output channel of the user's terminal
4. Set the output channel of the log buffer
5. Set the output channel of the log host
6. Display the information of the log channel
7. Set the filter items of the log output channel.

1. Set the global log switch

Command	Description
Privileged configuration mode	
logging on **no logging on**	Enable the global log function. Prefixing the command with a "no" will disable this function.

2. Set the output channel of the console

Command	Description
Privileged configuration mode	
logging console **no logging console**	Open the output channel of the console. Prefixing the command with a "no" will disable this function.

3.Set the output channel of the user's terminal

Command	Description
Privileged configuration mode	
logging monitor **no logging monitor**	Open the output channel of the user's terminal. Prefixing the command with a "no" will disable this function.

4.Set the output channel of the log buffer

Command	Description
Privileged configuration mode	
logging buffered [<*buffersize* >] **no logging buffered**	Open the output channel of the log buffer. Prefixing the command with a "no" will disable this function.
show logging buffered [< *buffersize* >]	Display detailed information of the channel of the log buffer
clear logging	Clear the information in the log buffer.

5.Set the output channel of the log host

Command	Description
Privileged configuration mode	
logging <*ip-addr*> [facility <*local-number*>] **no logging <*ip-addr*>**	Open the output channel of the log host. Prefixing the command with a “no” will disable this function.

6.Display the information of the log channel

Command	Description
Privileged configuration mode	
show channel [console | monitor | logbuff | loghost]	Display the information of the log channel

7.Set the filter items of the log output channel.

Command	Description
Privileged configuration mode	
logging source {<*modu-name*> | default } channel <*channel-name*> [level <severity> [state { on | off }]]	Add filter items to the output channel of the log.
no logging source { <*modu-name*> | default } channel <*channel-name*>	Delete filter items from the output channel of the log..

5.6.3 System Log Configuration Example

When managing VLAN the IPv4 address of the switch is 100.100.100.1, and the IPv4 address of the remote log server is 100.100.100.5. It is required to send the log information with a severity equal to or higher than warnings to this log server and save in the log record equipment local1, Output the log information of a module shell if its Severity Level is warning or critical.

configure
Switch(Config)#logging on↵
Switch(Config)#logging 100.100.100.5 facility local1↵
Switch(Config)#logging source m_shell channel loghost level debugging state on↵
Switch(Config)#logging source sys_event channel loghost level debugging state on↵
Switch(Config)#logging logbuffed 1000↵
Switch(Config)#logging source m_shell channel logbuff level warning state on↵

5.6.4 System Log troubleshooting

5.6.4.1 Monitor and Debug Command

5.6.4.1.1 show channel

Command show channel [console | monitor | logbuff | loghost]
Function To display brief information of the log channel.
Parameters console the output channel of log is console; monitor the output channel of log is the user's terminal; logbuff the output channel of log is the log buffer; loghost the output channel of log is the log host.
Command Mode Privileged configuration mode.
Default Setting show channel will display the brief information of all the channels without any parameter.
Relative Command logging on

5.6.4.1.2 show logging buffered

Command show logging buffered [<*buffersize*>]
Function To display detailed information of the channel of the log buffer
Parameters <*buffersize*> is the number of the log message to display
Command Mode Privileged configuration mode.
Default Setting 100 log messages will be displayed without any parameter.
Relative Command logging on，show channel logbuff

5.6.4.1.3 show logging lastFailureInfo

Command show logging lastFailureInfo
Function To display the abnormal information recorded in the flash
Command Mode Privileged configuration mode.
Relative Command erase logging lastFailureInfo

5.6.4.1.4 erase logging lastFailureInfo

Command erase logging lastFailureInfo
Function To erase the abnormal information recorded in the flash
Command Mode Privileged configuration mode.
Relative Command show logging lastFailureInfo

5.6.4.2 System Log troubleshooting

Please check the following causes if any problem happens when using the system log

- ✧ Check if the global log switch is on.
- ✧ Use the show channel command in the privileged mode to check the state of each channel and the state of the modules in filter items.

5.7 Classified Configuration

5.7.1 Introduction of Classified Configuration

In order to effectively protect the network, the switch allows users to log on as different identities to configure it, allows different password for those identities, and allows those identities to use different rights. when configuring the switch. Right now, DCN switch provides visitor and admin as configuration levels. Their differences is listed as follows

Identity to Log On	**Configuration Rights**
visitor	Most of show command and ping, traceroute, clear etc.. config mode is not allowed on this level
admin	All of the commands.

5.7.2 Configure the Classified Configuration

5.7.2.1 Configure the Task Sequence of the Classified Configuration

1. Command to enable privileged mode.
2. Set the corresponding password for the identity to log on.

1. Command to enable privileged mode

Command	**Explanation**
Enable [level { visitor | admin } [<*password*>]]	To log to the switch in the specified identity

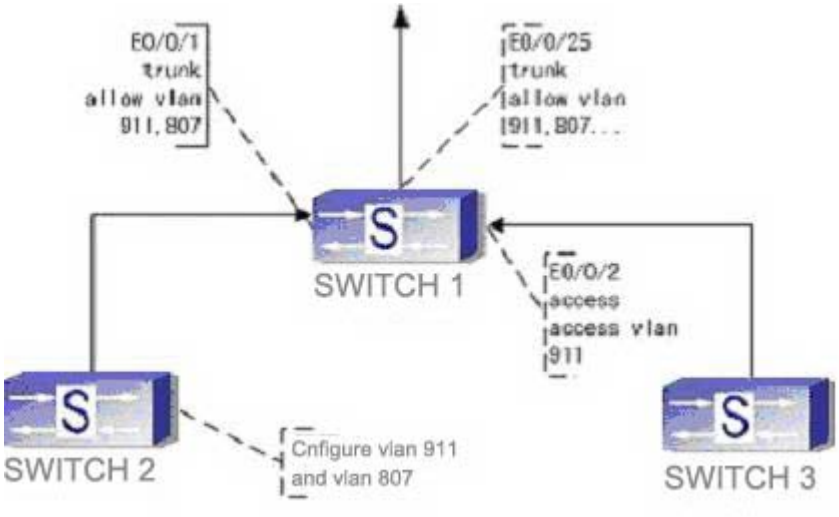
2. Set the corresponding password for the identity to log on.

Command	**Explanation**
enable password level {visitor|admin}	To set the password for logging to the configuration mode.

5.8 Port Isolation

5.8.1 Introduction of Port Isolation

Port isolation is aimed at meeting the user's demand showed below



The topologic structure of the switches is illustrated in the picture above. The demand is that, once the configuration port on switch1 is isolated, the e0/0/1 and e0/0/2 on switch1 are not connected, while both of which can be connected to the uplink port e0/0/25. That is all the downlink ports can not connect to each other, but a downlink port can be connected to a specified uplink port. The uplink port can be connected to any port.

5.8.2 Port Isolation Configuration

5.8.2.1 Task of port isolation configuration

1.Set the uplink port

Command	**Explanation**
isolate-port allowed ethernet <*InterfaceList*> **no isolate-port allowed [ethernet <*InterfaceList*>]**	Enable or disable the port isolation function. A uplink port list is needed to enable it. This command can be called more than once to set or cancel uplink ports.

Chapter 6 Cluster Configuration

6.1 Introduction to cluster network management

Cluster network management is an in-band configuration management. Unlike CLI, SNMP and Web Config which implement a direct management of the target switches through a management workstation, cluster network management implements a direct management of the target switches (member switches) through an intermediate switch (commander switch). A commander switch can manage multiple member switches. As soon as a Public IP address is configured in the commander switch, all the member switches which are configured with private IP addresses can be managed remotely. This feature economizes public IP addresses which are short of supply. Cluster network management can dynamically discover cluster feature enabled switches (candidate switches). Network administrators can statically or dynamically add the candidate switches to the cluster which is already established. Accordingly, they can configure and manage the member switches through the commander switch. When the member switches are distributed in various physical locations (such as on the different floors of the same building), cluster network management has obvious advantages. Moreover, cluster network management is an in-band management. The commander switch can communicate with member switches in existing network. There is no need to build a specific network for network management.

Cluster network management has the following features

- Save IP addresses
- Simplify configuration tasks
- Indifference to network topology and distance limitation
- Auto detecting and auto establishing
- With factory default settings, multiple switches can be managed through cluster network management
- The commander switch can upgrade and configure any member switches in the cluster

6.2 Cluster Network Management Configuration

6.2.1 Cluster Network Management Configuration Sequence

1. Enable or disable cluster function
2. Create cluster
   1) Create or delete cluster
   2) Configure private IP address pool for member switches of the cluster
   3) Add or remove a member switch
3. Configure attributes of the cluster in the commander switch

1) Enable or disable joining the cluster automatically
2) Set holdtime of heartbeat of the cluster
3) Set interval of sending heartbeat packets among the switches of the cluster
4) Clear the list of candidate switches discovered by the commander switch

4. Configure attributes of the cluster in the candidate switch
   1) Set interval of sending cluster register packet
5. Remote cluster network management
   1) Remote configuration management
   2) Reboot member switch
   3) Remotely upgrade member switch

1.Enable or disable cluster

Command	Explanation
Global Mode	
cluster run **no cluster run**	Enable or disable cluster function in the switch

2. Create a cluster

Command	Explanation
Global Mode	
cluster commander <*cluster-name*> ***[vlan<vlan-id>]*** **no cluster commander**	Create or delete a cluster
cluster ip-pool<*commander-ip*> **no cluster ip-pool**	Configure private IP address pool for member switches of the cluster
cluster member {candidate-sn <*cand-sn*> | mac-address <*mac-add*> [<*mem-id*>] }[password <*pass*>] **no cluster member < *mem-id* >**	Add or remove a member switch

3. Configure attributes of the cluster in the commander switch

Command	Explanation
Global Mode	
cluster auto-add enable **no cluster auto-add enable**	Enable or disable adding newly discovered candidate switch to the cluster
cluster holdtime < second> **no cluster holdtime**	Set holdtime of heartbeat of the cluster
cluster heartbeat <*interval*> **no cluster heartbeat**	Set interval of sending heartbeat packets among the switches of the cluster
clear cluster candidate-table	Clear the list of candidate switches discovered by the commander switch

4. Configure attributes of the cluster in the candidate switch

Command	Explanation

Global Mode	
cluster register timer <*timer-value*> **no cluster register timer**	Set interval of sending cluster register packet

5. Remote cluster network management

Command	**Explanation**
Admin Mode	
rcommand member <mem-id>	In the commander switch, this command is used to configure and manage member switches.
rcommand commander	In the member switch, this command is used to configure the member switch itself.
cluster reset member<mem-id>	In the commander switch, this command is used to reset the member switch.
cluster update member <*mem-id*> <*src-url*> <*dst-url*> [ascii | binary]	In the commander switch, this command is used to remotely upgrade the member switch.

Chapter 7 Port Configuration

7.1 Port Introduction

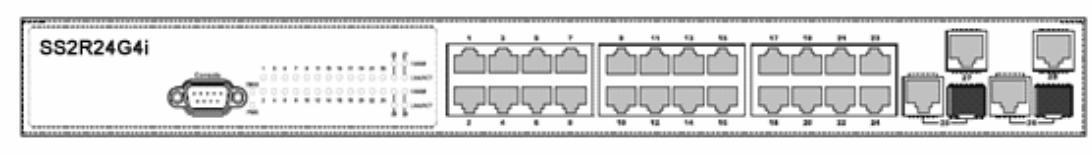


Fig 7-1 Ports on SS2R24G4i

The ports on SS2R24G4i switch are showed in the above picture. SS2R24G4i provides 24＋2＋2 ports, 24 of wich are 10/100Base-TX ethernet interfaces with fixed configuration, 2 of which are 1000Base-TX/1000Base-FX single/multi mode interfaces, the other 2 of which are 1000Base-TX stack interfaces.

On the panel of SS2R24G4I, each port is marked with a port ID. The relationshipbetween these port IDs and the port IDs provided by the SS2R24G4I operating system (software port IDs)is listed as follows

Physical port ID	**Software port ID**
24 10/100Base-T	ethernet 0/0/1-24
2 1000Base-TX/1000Base-FX	ethernet 0/0/25-26
2 1000Base-TX	ethernet 0/0/27-28

If users want to configure some ports, they can use the command **interface ethernet *<interface-list>*** to enter corresponding ethernet port configuration mode, the parameter ***<interface-list>*** can be 0/0/1-28. When ***<interface-list>*** contains more than one ports, please use special charactuer including";"and "-" to connect them. In the ethernet port configuration mode, the port rate, duplex mode and the traffic control can all be configured, in response, the performace of corresponding ports will change accordingly.

7.2 Port Configuration

7.2.1 Port Configuration

7.2.1.1 Port Configuration Task List

1. Enter the network port configuration mode
2. Configure the properties for the network ports
   1) Configure combo mode for combo ports
   2) Enable/Disable ports
   3) Configure port names

4) Configure port cable types
5) Configure port speed and duplex mode
6) Configure bandwidth control
7) Configure traffic control
8) Enable/Disable port loopback function
9) Configure Combo port mode

3. Set the packet suppression function

1. Enter the Ethernet port configuration mode

Command	Explanation
Interface Mode	
interface ethernet <*interface-list*>	Enters the network port configuration mode.

2. Configure the properties for the Ethernet ports

Command	Explanation
Interface Mode	
shutdown **no shutdown**	Enables/Disables specified ports
name <*string*> **no name**	Names or cancels the name of specified ports
mdi { auto | across | normal } **no mdi**	Sets the cable type for the specified port
speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | force100-fx | {{force1g-half | force1g-full} [nonegotiate [master | slave]] } }	Sets port speed and duplex mode
bandwidth control <*bandwidth*> [transmit] **no bandwidth control**	Sets receive/send data bandwidth on specified ports
flow control **no flow control**	Enables/Disables traffic control function for specified ports
loopback **no loopback**	Enables/Disables loopback test function for specified ports
combo-forced-mode {copper-forced | copper-prefered-auto | sfp-forced | sfp-prefered-auto } **no combo-forced-mode**	Sets combo port mode

3.Set the packet suppression function

Command	Explanation
Port configuration mode	
packet-suppression <*packets*> {broadcast|brmc|brmcdlf|all} **no packet-suppression**	Enable the packet suppresntion function of the switch, and set the max data traffic allowed to pass. The "no packet-suppression" command is used to cancel the packet suppression function.

7.2.2 VLAN Interface Configuration

7.2.2.1 VLAN Interface Configuration Task List

1. Enter VLAN Mode
2. Configure the IP address for VLAN interface and enable VLAN interface.

1. Enter VLAN Mode

Command	Explanation
Global Mode	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	Enters VLAN Interface Mode; the "**no interface vlan <*vlan-id*>**" command deletes specified VLAN interface.

2. Configure the IP address for VLAN interface and enables VLAN interface.

Command	Explanation
VLAN Mode	
ip address <*ip-address*> <*mask*> [secondary] **no ip address [<*ip-address*> <*mask*>]**	Configures the VLAN interface IP address; the "**no ip address [<*ip-address*> <*mask*>]"** command deletes the VLAN interface IP address.
VLAN Mode	
Shutdown **no shutdown**	Enables/Disables VLAN interface

7.2.3 Port Mirroring Configuration

7.2.3.1 Introduction to Port Mirroring

Port mirroring refers to the duplication of data frames sent/received on a port to another port. The duplicated port is referred to as mirror source port and the duplicating port is referred to as mirror destination port. A protocol analyzer (such as Sniffer) or RMON monitoring instrument is often attached to the mirror destination port to monitor and manage the network and diagnostic.

SS2R24/48G4i switch switch support one mirror destination port only. The number of mirror source ports are not limited, one or more may be used. Multiple source ports can be within the same VLAN or across several VLANs. The destination port and source port(s) can be located in different VLANs.

7.2.3.2 Port Mirroring Configuration Task List

1. Specify mirror source port
2. Specify mirror dentistination port

1. Specify mirror source port

Command	**Explanation**
Port mode	
monitor session <*session*> source interface <*interface-list*> {rx | tx | both} **no monitor session <*session*> source interface <*interface-list*>**	Specify mirror source port, the **no monitor session <*session*> source interface <*interface-list*>** command deletes mirror source port

2. Specify mirror dentistination port

Command	**Explanation**
Port mode	
monitor session <*session*> destination interface <*interface-number*> **no monitor session <*session*> destination interface <*interface-number*>**	Specify mirror dentistination port;the **no monitor session <*session*> destination interface <*interface-number*>** command deletes mirror dentistination port

7.2.3.3 Mirror Port Examples

Port configuration Examples

7.2.3.4 Device Mirroring Troubleshooting

7.2.3.4.1 show monitor

Command show monitor
Function To display the source and destination port information of the image.
Command Mode Admin Mode

Display information	Explanation
session number	Session number of the image
Source ports	Source ports of the image
RX	The image in the receiving direction of the port.
TX	The image in the transmitting direction of the port.
Both	The images in both the receiving and transmitting directions of the port.
Destination port	Destination port of the image

7.2.3.4.2 debug mirror

Command debug mirror
no debug mirror
Function
To enable the debug information of the mirror, the “no debug mirror”command is used to disable the debug information of the mirror.
Command Mode Admin Mode

7.2.3.4.3 Device Mirroring Troubleshooting

If problems occurs on configuring port mirroring, please check the following first for causes

- ☞ Whether the mirror destination port is a member of a trunk group or not, if yes, modify the trunk group.
- ☞ If the throughput of mirror destination port is smaller than the total throughput of mirror source port(s), the destination port will not be able to duplicate all source port traffic; please decrease the number of source ports, duplicate traffic for one direction only or choose a port with greater throughput as the destination port.

7.3 Port Configuration Example

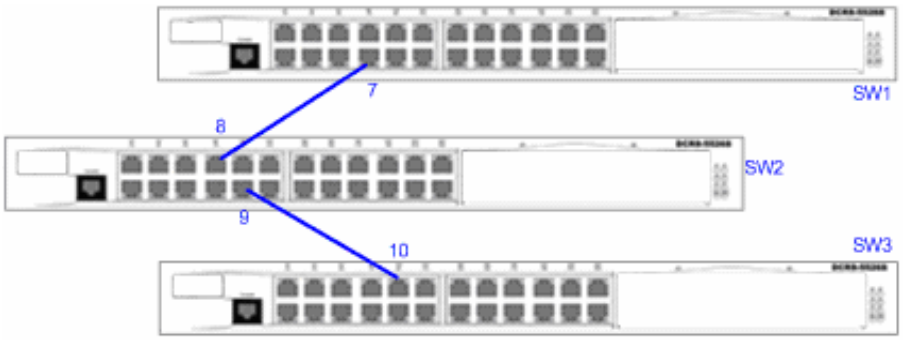


Fig 7-2 Port Configuration Example

Use default VLAN1 since VLAN is not configured on all of the switches.

Switch	Port	Attributes
SW1	0/0/7	10M/full
SW2	0/0/8-9	10M/full,mirror source port
	0/0/24	100M/full,mirror dentistination port
SW3	0/0/10	10M/full

The configurations are listed below

SW1

Switch1(Config)#interface ethernet 0/0/7

Switch1(Config-Ethernet0/0/7)#speed-duplex force10-full

SW2

Switch2(Config)#interface ethernet 0/0/8-9

l

Switch2(Config-Port-Range)#speed-duplex force10-full

Switch2(Config-Port-Range)#exit

Switch2(Config)#interface ethernet 0/0/24

Switch2(Config-Ethernet0/0/24)#speed-duplex force100-full

Switch2(Config-Ethernet0/0/24)#exit

Switch2(Config)#monitor session 1 source interface ethernet 0/0/8-9

Switch2(Config)#monitor session 1 destination interface ethernet 0/0/24

SW3

Switch3(Config)#interface ethernet 0/0/10

Switch3(Config-Ethernet0/0/10)#speed-duplex force10-full

7.4 Port Troubleshooting

7.4.1 Monitor and Debug Command

7.4.1.1 clear counters ethernet

Command clear counters [ethernet <*interface-list*>]
Function Clear counters information on Ethernet interface
Parameters <*interface-list*>is the port ID of Ethernet
Command Mode Admin Mode
Default Do not delete the counters information on Ethernet interface

7.4.1.2 show interface ethernet

Command show interface ethernet <*interface-list*>
Function To display the information of the ports on the specified switch.
Parameters <*interface-list*>is the port ID, the format and value range of the port ID is explained in the port introduction part of this chapter.
Command Mode Admin Mode

Chapter 8 MAC Table Configuration

8.1 Introduction to MAC Table

MAC table is a table identifies the mapping relationship between destination MAC addresses and switch ports. MAC addresses can be categorized as static MAC addresses and dynamic MAC addresses. Static MAC addresses are manually configured by the user, have the highest priority and are permanently effective (will not be overwritten by dynamic MAC addresses); dynamic MAC addresses are entries learnt by the switch in data frame forwarding, and is effective for a limited period. When the switch receives a data frame to be forwarded, it stores the source MAC address of the data frame and creates a mapping to the destination port. Then the MAC table is queried for the destination MAC address, if hit, the data frame is forwarded in the associated port, otherwise, the switch forwards the data frame to its broadcast domain. If a dynamic MAC address is not learnt from the data frames to be forwarded for a long time, the entry will be deleted from the switch MAC table.
There are two MAC table operations

1. Obtain a MAC address;
2. Forward or filter data frame according to the MAC table.

8.1.1 Obtaining MAC Table

The MAC table can be built up staticly and dynamically. Static configuration is to set up a mapping between the MAC addresses and the ports; dynamic learning is the process in which the switch learns the mapping between MAC addresses and ports, and updates the MAC table regularly. In this section, we will focus on the dynamic learning process of MAC table.

The topology of the figure above 4 PCs connected to SS2R24/48G4i switch switch, where PC1 and PC2 belongs to a same physical segment (same collision domain), the physical segment connects to port 5 of SS2R24/48G4i switch switch; PC3 and PC4 belongs to the same physical segment that connects to port 12 of SS2R24/48G4i switch switch.

The initial MAC table contains no address mapping entries. Take the communication of PC1 and PC3 as an example, the MAC address learning process is as follow

1. When PC1 sends message to PC3, the switch receives the source MAC address 00-01-11-11-11-11 from this message, the mapping entry of 00-01-11-11-11-11 and port 5 is added to the switch MAC table.
2. At the same time, the switch learns the message is destined to 00-01-33-33-33-33, as the MAC table contains only a mapping entry of MAC address 00-01-11-11-11-11 and port 5, and no port mapping for 00-01-33-33-33-33 present, the switch broadcast this message to all the ports in the switch (assuming all ports belong to the default VLAN1).
3. PC3 and PC4 on port 12 receive the message sent by PC1, but PC4 will not reply, as the destination MAC address is 00-01-33-33-33-33, only PC3 will reply to PC1. When port 12 receives the message sent by PC3, a mapping entry for MAC address 00-01-33-33-33-33 and port 12 is

added to the MAC table.

4. Now the MAC table has two dynamic entries, MAC address 00-01-11-11-11-11 - port 5 and 00-01-33-33-33-33 -port 12.
5. After the communication between PC1 and PC3, the switch does not receive any message sent from PC1 and PC3. And the MAC address mapping entries in the MAC table are deleted after 300 seconds. The 300 seconds here is the default aging time for MAC address entry in SS2R24/48G4i switch. Aging time can be modified in the switch.

8.1.2 Forward or Filte

The switch will forward or filter received data frames according to the MAC table. Take the above figure as an example, assuming DCN switch have learnt the MAC address of PC1 and PC3, and the user manually configured the mapping relationship for PC2 and PC4 to ports. The MAC table of DCN switch will be

MAC Address	Port number	Entry added by
00-01-11-11-11-11	5	Dynamic learning
00-01-22-22-22-22	5	Static configuration
00-01-33-33-33-33	12	Dynamic learning
00-01-44-44-44-44	12	Static configuration

- Forward data according to the MAC table
  If PC1 sends a message to PC3, the switch will forward the data received on port 5 from port 12.
- Filter data according to the MAC table
  If PC1 sends a message to PC2, the switch, on checking the MAC table, will find PC2 and PC1 are in the same physical segment and filter the message (i.e. drop this message).

Three types of frames can be forwarded by the switch

- Broadcast frame
- Multicast frame
- Unicast frame

The following describes how the switch deals with all the three types of frames

1. Broadcast frame The switch can segregate collision domains but not broadcast domains. If no VLAN is set, all devices connected to the switch are in the same broadcast domain. When the switch receives a broadcast frame, it forwards the frame in all ports. When VLANs are configured in the switch, the MAC table will be adapted accordingly to add VLAN information. In this case, the switch will not forward the received broadcast frames in all ports, but forward the frames in all ports in the same VLAN.
2. Multicast frame When IGMP Snooping function is not enabled, multicast frames are processed in the same way as broadcast frames; when IGMP Snooping is enabled, the switch will only forward the multicast frames to the ports belonging to the very multicast group.
3. Unicast frame When no VLAN is configured, if the destination MAC addresses are in the switch MAC table, the switch will directly forward the frames to the associated ports; when the destination MAC address in a unicast frame is not found in the MAC table, the switch will broadcast the unicast

frame. When VLANs are configured, the switch will forward unicast frame within the same VLAN. If the destination MAC address is found in the MAC table but belonging to different VLANs, the switch can only broadcast the unicast frame in the VLAN it belongs to.

8.2 Commands for MAC address table configuration

8.2.1 mac-address-table aging-time

Command mac-address-table aging-time {<*age*> | 0}

no mac-address-table aging-time

Function Set the aging time for address mapping entries in the MAC table dynamically learnt; the "**no mac-address-table aging-time**" command restores the aging time to the default 300 seconds.

Parameter **< *age*>** is the aging time in seconds, the valid range is 10 to 100000; 0 for no aging.

Command mode Global Mode

Default The system default aging time is 300 seconds.

8.2.2 mac-address-table

Command mac-address-table static address <*mac-addr*> vlan <*vlan-id* > interface [Ethernet|port-channel]<*interface-name*>

no mac-address-table [static |dynamic] [address <*mac-addr*>] [vlan <*vlan-id*>] [interface <*interface-name*>]

Function Add or modify static address entries, The "**no mac-address-table [static |dynamic] [address <*mac-addr*>] [vlan <*vlan-id*>] [interface <*interface-name*>"** command deletes the static,dynamic and mac address table entries.

Parameter static is the static entries; **<*mac-addr*>** MAC address to be added or deleted;**<*interface-name*>** name of the port transmitting the MAC data packet;**<*vlan-id*>** is the vlan number.

Command Mode Global mode

Default When VLAN or Layer 3 interface is configured and is up, the system will generate an static address mapping entry of which the inherent MAC address corresponds to the VLAN or Layer 3 interface.

8.2.3 mac-address-table blackhole

Command mac-address-table blackhole address <*mac-addr*> vlan <*vlan-id* >

no mac-address-table blackhole [address <*mac-addr*>] [vlan <*vlan-id*>]

Function Add or modify filtering address entries,the "**no mac-address-table blackhole [address <*mac-addr*>] [vlan <*vlan-id*>]" deletes** filtering address entries.

Parameter <*mac-addr*> MAC address to be added or deleted; **<*vlan-id*>** receives vlan number of the MAC data packet

Command Mode Global mode
Default no filtering entries

8.2.4 clear mac-address-table dynamic

Command clear mac-address-table dynamic [address <*hw_addr*>] [vlan <*vid*>] [interface {[ethernet|port-channel] <*Interfacename*>}]
Function Deletes dynamic address entries
Parameter <*mac-addr*> MAC address to be deleted; **<*interface-name*>** name of the port transmitting the MAC data packet; **<*vlan-id*>** receives vlan number of the MAC data packet.
Command Mode Admin mode
Default None

8.3 Typical Configuration Example

Scenario Four PCs as shown in the above figure connect to port 5, 7, 9, 11 of switch, all the four PCs belong to the default VLAN1. As required by the network environment, dynamic learning is enabled. PC1 holds sensitive data and can not be accessed by any other PC that is in another physical segment; PC2 and PC3 have static mapping set to port 7 and port 9, respectively.

The configuration steps are listed below

1. Set the MAC address 00-01-11-11-11-11 of PC1 as a filter address.
Switch(Config)#mac-address-table blackhole address 00-01-11-11-11-11 vlan 1
2.Set the static mapping relationship for PC2 and PC3 to port 7 and port 9, respectively.
Switch(Config)#mac-address-table static address 00-01-22-22-22-22 vlan 1 interface ethernet 0/0/7
Switch(Config)#mac-address-table static address 00-01-33-33-33-33 vlan 1 interface ethernet 0/0/9

8.4 Troubleshooting

8.4.1 Monitor and Debug Command

8.4.1.1 show mac-address-table

Command show mac-address-table [static|aging-time|blackhole|count] [address <*mac-addr*>] [vlan <*vlan-id*>] [interface <*interface-name*>]
Parameter static entry; **aging-time** address aging time; **blackhole** filtering entry; **count** address counter; **<*mac-addr*>** entry's MAC address; **<*vlan-id*>** entry's VLAN number; **<*interface-name*>** entry's interface name
Command mode Admin mode
Default MAC address table is not displayed by default.

8.4.2 Troubleshooting

Using the show mac-address-table command, a port is found to be failed to learn the MAC of a device connected to it. Possible reasons

- The connected cable is broken.
- Spanning Tree is enabled and the port is in “discarding” status; or the device is just connected to the port and Spanning Tree is still under calculation, wait until the Spanning Tree calculation finishes, and the port will learn the MAC address.
- If not the problems mentioned above , please check for the switch portand contact technical support for solution.

8.5 MAC Address Function Extension

8.5.1 MAC Address Binding

8.5.1.1 Introduction to MAC Address Binding

Most switches support MAC address learning, each port can dynamically learn several MAC addresses, so that forwarding data streams between known MAC addresses within the ports can be achieved. If a MAC address is aged, the packet destined for that entry will be broadcasted. In other words, a MAC address learned in a port will be used for forwarding in that port, if the connection is changed to another port, the switch will learn the MAC address again to forward data in the new port.

However,in some cases, security or management policy may require MAC addresses to be bound with the ports, only data stream from the binding MAC are allowed to be forwarded in the ports. That is to say, after a MAC address is bound to a port, only the data stream destined for that MAC address can flow in from the binding port, data stream destined for the other MAC addresses that not bound to the port will not be allowed to pass through the port.

8.5.1.2 MAC Address Binding Configuration

8.5.1.2.1 MAC Address Binding Configuration Task List

1.Enable MAC address binding function for the ports
2.Lock the MAC addresses for a port
3.MAC address binding property configuration

1. Enable MAC address binding function for the ports

Command	Explanation
Interface Mode	
switchport port-security **no switchport port-security**	Enable MAC address binding function;the" **no switchport port-security** command disables the MAC address binding function

2. Lock the MAC addresses for a port

Command	Explanation
Interface Mode	
switchport port-security lock **no switchport port-security lock**	Lock the port. After locking the port, no MAC address can be learnt. "**no switchport port-security lock**" resume the MAC address learning.
switchport port-security convert	Convert dynamic secure MAC addresses learned by the port to static secure MAC addresses.
switchport port-security timeout <*value*> **no switchport port-security timeout**	Enable port locking timer function; the "**no switchport port-security timeout**" restores the default setting.
switchport port-security mac-address <*mac-address*> **no switchport port-security mac-address <*mac-address*>**	Add static secure MAC address; the "**no switchport port-security mac-address <*mac-address*>"** command deletes static secure MAC address.
clear port-security dynamic [address <*mac-addr*> | interface <*interface-id*>]	Clear dynamic MAC addresses learned by the specified port.

3. MAC address binding property configuration

Command	Explanation
Interface Mode	
switchport port-security maximum <*value*> **no switchport port-security maximum <*value*>**	Set the maximum number of secure MAC addresses for a port; the "**no switchport port-security maximum <*value*>**" command restores the default value.
switchport port-security violation {protect | shutdown} **no switchport port-security violation**	Set the violation mode for the port; the " **no switchport port-security violation** " command restores the default setting.

8.5.1.3 MAC Address Binding Troubleshooting

8.5.1.3.1 MAC Address Binding Monitor and Debug Comman

8.5.1.3.2 show port-security

Command show port-security
Function Display the secure MAC addresses of the port.
Command mode Admin Mode
Parameter ***<interface-list>*** stands for the port to be displayed.

Displayed information	Explanation
Security Port	Configure port name of Security Port
MaxSecurityAddr	MAC Configure maximum of security address number of Security Port
CurrentAddr	Current secure MAC address number of Security Port
Security Action	Violation mode of port configuration
Total Addresses in System	Current secure MAC address number in the system.
Max Addresses limit in System	Maximum in addresses limit in system

8.5.1.3.3 show port-security interface

Command show port-security interface *<interface-id>*
Function Display the secure MAC addresses of the port.
Command mode Admin Mode
Parameter ***<interface-id>***stands for the port to be displayed
Default Configuration of Security Port is not be displayed

Displayed information	Explanation
Port Security	Enable to be Port Security or not
Port status	Port Security status
Violation mode	Violation mode of port setup
Maximum MAC Addresses	Maximum MAC Addresses of port setup
Total MAC Addresses	Current total MAC addresses of port setup
Configured MAC Addresses	Security MAC Addresses of port static configuration
Lock Timer	Enable lock timer or not on the port
Mac-Learning function	Enable Mac-learning function or not

8.5.1.3.4 show port-security address

Command show port-security address [interface <*interface-id*>]
Function Display the secure MAC addresses of the port.
Command mode Admin Mode
Parameter ***<interface-id>*** stands for the port to be displayed.

Displayed information	Explanation
Vlan	The VLAN ID for the secure MAC Address
Mac Address	Secure MAC address
Type	Secure MAC address type
Ports	The port that the secure MAC address belongs to
Total Addresses	Current secure MAC address number in the system.

8.5.1.3.5 Binding MAC Address Binding Troubleshootin

Enabling MAC address binding for ports may fail in some occasions. Here are some possible causes and solutions

- If MAC address binding cannot be enabled for a port, make sure the port is not enabling Spanning tree or port aggregation and is not configured as a Trunk port. MAC address binding is exclusive to such configurations. If MAC address binding is to be enabled, the functions mentioned above must be disabled first
- If a secure address is set as static address and deleted, that secure address will be unusable even though it exists. For this reason, it is recommended to avoid static address for ports enabling MAC addres
- Users might find that some deviced connected to the ports configured with MAC address binding fucntion can not transimit data. If so, please check whether the MAC addresses of these devices has been transformed into secure MAC, if not, even the switch has learnt the MAC addresses of these devices, they can not transmit data, because only secure MAC can transmit data when the ports has enabled the MAC address binding function

Chapter 9 VLAN Configuration

9.1 Introduction to VLAN

VLAN (Virtual Local Area Network) is a technology that divides the logical addresses of devices within the network to separate network segments basing on functions, applications or management requirements. By this way, virtual workgroups can be formed regardless of the physical location of the devices. IEEE announced IEEE 802.1Q protocol to direct the standardized VLAN implementation, and the VLAN function of the switch is implemented following IEEE 802.1Q.

The key idea of VLAN technology is that a large LAN can be partitioned into many separate broadcast domains dynamically to meet the demands.

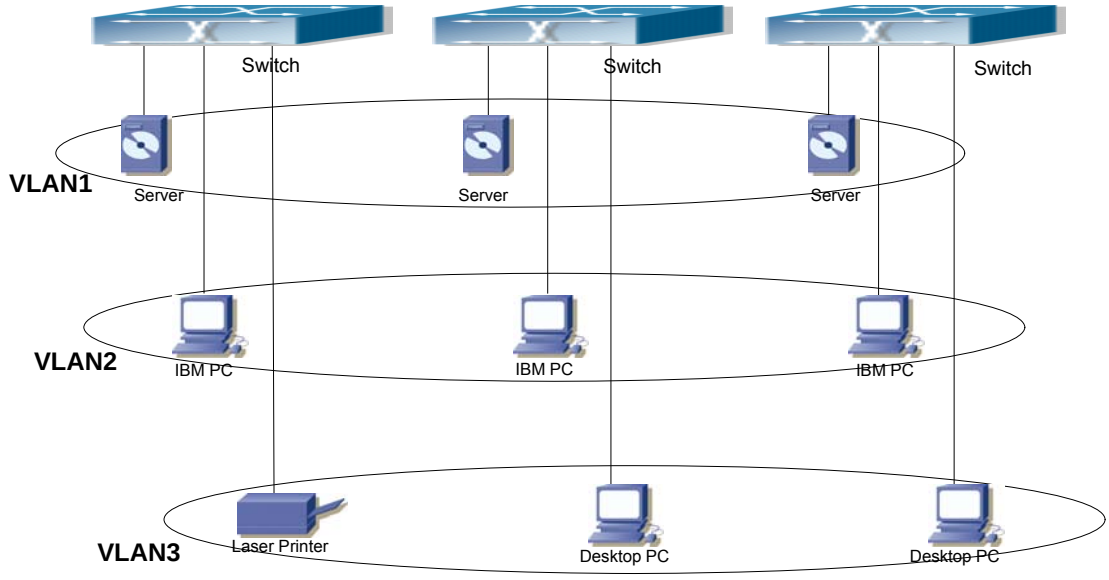


Fig 9-1 A VLAN network defined logically

Each broadcast domain is a VLAN. VLANs have the same properties as the physical LANs, except VLAN is a logical partition rather than physical one. Therefore, the partition of VLANs can be performed regardless of physical locations, and the broadcast, multicast and unicast traffic within a VLAN is separated from the other VLANs.

With the aforementioned features, VLAN technology provides us with the following convenience

- Improving network performance
- Saving network resources
- Simplifying Network Management
- Lowering network cost
- Enhancing network security

VLAN and GVRP (GARP VLAN Registration Protocol) defined by 802.1Q are implemented in SS2R24/48G4i switch switch. The chapter will describe the use and configuration of VLAN and GVRP in details.

9.2 VLAN Configuration

9.2.1 VLAN Configuration Task List

1. Creating or deleting VLAN
2. Specifying or deleting name of VLAN
3. Assigning Switch ports for VLAN
4. Set The Switch Port Type
5. Set Trunk port
6. Set Access port
7. Enable/Disable VLAN ingress rules on ports
8. Configure Private VLAN
9. Set Private VLAN association

1. Creating or deleting VLAN

Command	**Explanation**
Global Mode	
vlan <*vlan-id*> **no vlan <*vlan-id*>**	Create/delete VLAN or enter VLAN Mode

2.Specifying or deleting name of VLAN

Command	**Explanation**
Global Mode	
name <*vlan-name*> **no name**	Specifying or deleting name of VLAN

3. Assigning Switch ports for VLAN

Command	**Explanation**
VLAN Mode	
switchport interface <*interface-list*> **no switchport interface <*interface-list*>**	Assign Switch ports to VLAN

4. Set The Switch Port Type

Command	Explanation
Interface Mode	
switchport mode {trunk|access}	Set the current port as Trunk or Access port.

5. Set Trunk port

Command	Explanation
Interface Mode	
switchport trunk allowed vlan {<*vlan-list*>|all} **no switchport trunk allowed vlan <*vlan-list*>**	Set/delete VLAN allowed to be crossed by Trunk. The "no" command restores the default setting.
switchport trunk native vlan <*vlan-id*> **no switchport trunk native vlan**	Set/delete PVID for Trunk port.

6.Set Access port

Command	Explanation
Interface Mode	
switchport access vlan <*vlan-id*> **no switchport access vlan**	Add the current port to specified VLAN the specified VLANs.

7. Disable/Enable VLAN Ingress Rules

8

Command	Explanation
Global Mode	
switchport ingress-filtering **no switchport ingress-filtering**	Disable/Enable VLAN ingress rules

Configure Private VLAN

Command	Explanation
VLAN mode	
private-vlan {primary|isolated|community} **no private-vlan**	Configure current VLAN to Private VLAN

9. Set Private VLAN association

Command	Explanation
VLAN mode	
private-vlan association <*secondary-vlan-list*> **no private-vlan association**	Set/delete Private VLAN association

9.2.2 Typical VLAN Application

Scenario

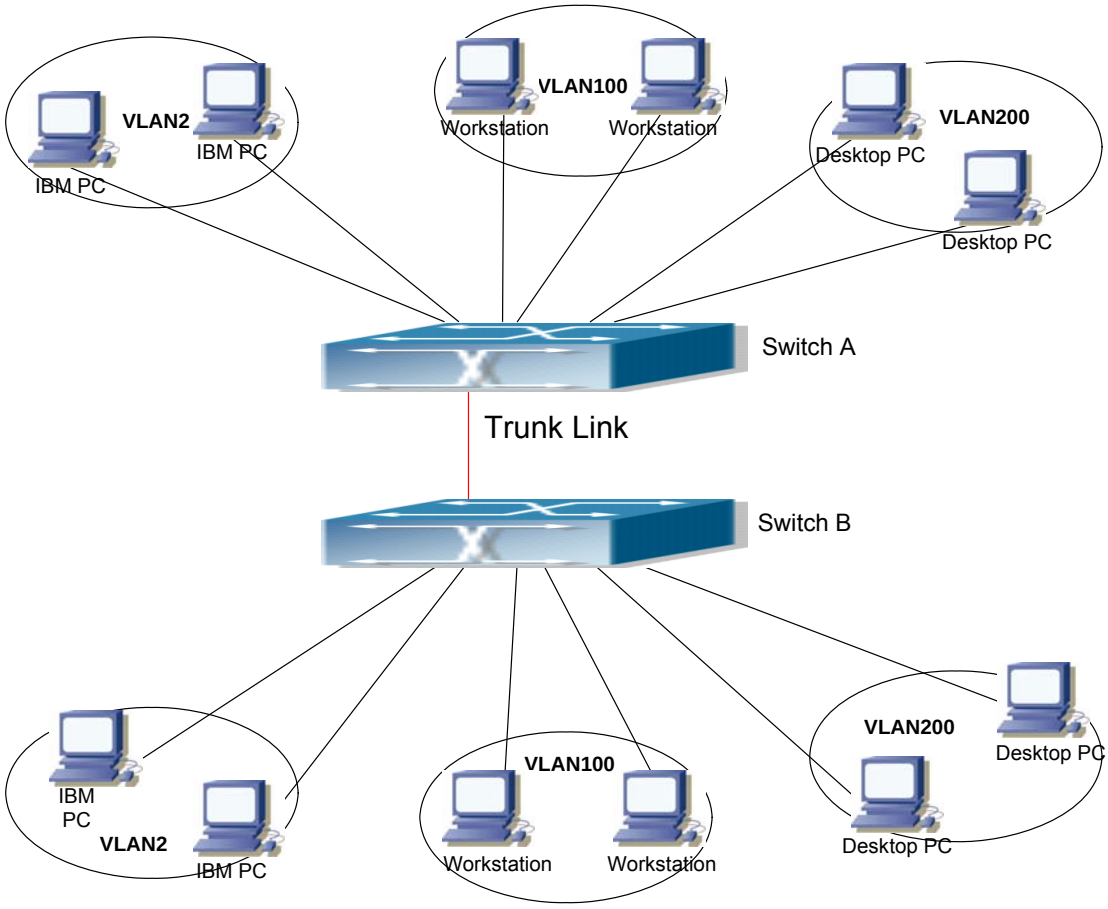


Fig 9-2 Typical VLAN Application Topology

The existing LAN is required to be partitioned to 3 VLANs due to security and application requirements. The three VLANs are VLAN2, VLAN100 and VLAN200. Those three VLANs are cross two different location A and B. One switch is placed in each site, and cross-location requirement can be met if VLAN traffic can be transferred between the two switches.

Configuration Item	**Configuration description**
VLAN2	Site A and site B switch port 2 -8.
VLAN100	Site A and site B switch port 9 -15.
VLAN200	Site A and site B switch port 16 -22.
Trunk port	Site A and site B switch port 23.

Connect the Trunk ports of both switches for a Trunk link to convey the cross-switch VLAN traffic; connect all network devices to the other ports of corresponding VLANs.
In this example, port 1 and port 24 is spared and can be used for management port or for other purposes.

The configuration steps are listed below
Switch A
Switch(Config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 0/0/2-8
Switch(Config-Vlan2)#exit
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 0/0/9-15
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 0/0/16-22
Switch(Config-Vlan200)#exit
Switch(Config)#interface ethernet 0/0/23
Switch(Config-Ethernet0/0/23)#switchport mode trunk
Switch(Config-Ethernet0/0/23)#exit
Switch(Config)#
Switch B
Switch(Config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 0/0/2-8
Switch(Config-Vlan2)#exit
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 0/0/9-15
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 0/0/16-22
Switch(Config-Vlan200)#exit
Switch(Config)#interface ethernet 0/0/23
Switch(Config-Ethernet0/0/23)#switchport mode trunk
Switch(Config-Ethernet0/0/23)#exit

9.3 Dot1q-tunnel Configuration

9.3.1 Dot1q-tunnel Introduction

Dot1q-tunnel is also called QinQ (802.1Q-in-802.1Q), which is an expansion of 802.1Q. Its dominating idea is encapsulating the customer VLAN tag (CVLAN tag) to the service provider VLAN tag (SPVLAN tag). Carrying the two VLAN tags the packet is transmitted through the backbone network of the ISP internet, so to provide a simple layer-2 tunnel for the users. It is simple and easy to manage, applicable only by static configuration, and especially adaptive to small office network or small scale

metropolitan area network using layer-3 switch as backbone equipment.

As shown in Fig 5-4, after being enabled on the user port, dot1q-tunnel assigns each user an SPVLAN identification (SPVID). Here the identification of user is 3. Same SPVID should be assigned for the same network user on different PEs. When packet reaches PE1 from CE1, it carries the VLAN tag 200-300 of the user internal network. Since the dot1q-tunnel function is enabled, the user port on PE1 will add on the packet another VLAN tag, of which the ID is the SPVID assigned to the user. Afterwards, the packet will only be transmitted in VLAN3 when traveling in the ISP internet network while carrying two VLAN tags (the inner tag is added when entering PE1, and the outer is SPVID), whereas the VLAN information of the user network is open to the provider network. When the packet reaches PE2 and before being forwarded to CE2 from the client port on PE2, the outer VLAN tag is removed, then the packet CE2 receives is absolutely identical to the one sent by CE1. For the user, the role the operator network plays between PE1 and PE2,is to provide a reliable layer-2 link.

The technology of Dot1q-tuunel provides the ISP internet the ability of supporting many client VLANs by only one VLAN of theirselves. Both the ISP internet and the clients can configure their own VLAN independently.

It is obvious that, the dot1q-tunnel function has got following characteristics

- Applicable through simple static configuration, no complex configuration or maintenance to be needed.
- Operators will only have to assign one SPVID for each user, which increases the number of concurrent supportable users; while the users has got the ultimate freedom in selecting and managing the VLAN IDs (select within 1~4096 at users' will).
- The user network is considerably independent. When the ISP internet is upgrading their network, the user networks do not have to change their original configuration.

Detailed description on the application and configuration of dot1q-tunnel of SS2R24/48G4i switch will be provided in this section

9.3.2 Configuration Task Sequence Of Dot1q-Tunnel

1. Configure the dot1q-tunnel function on the ports
2. Configure the type of protocol (TPID) on the ports
3. Configure the dot1q-tunnel type of the port.

1.Configure the dot1q-tunnel function on the ports

Command	**Explanation**
Port mode	
dot1q-tunnel enable **no dot1q-tunnel enable**	Enter/exit the dot1q-tunnel mode on the ports.

2. Configure the type of protocol (TPID) of the port

Command	Explanation
Port mode	
dot1q-tunnel tpid {8100|9100|9200}	Configure the type of protocol on the ports.

3.Set the dot1q-tunnel type of the port

Command	Explanation
Interface configuraiton mode	
switchport dot1q-tunnel mode {customer |uplink} **no switchport dot1q-tunnel**	Set the dot1q-tunnel type of the port

9.3.3 Typical Applications Of The Dot1q-tunnel

Scenario

Edge switch PE1 and PE2 of the ISP internet forward the VLAN200~300 data between CE1 and CE2 of the client network with VLAN3. The port1 of PE1 is connected to CE1, port10 is connected to public network, the TPID of the connected equipment is 9100; port1 of PE2 is connected to CE2, port10 is connected to public network

Configuration Item	Configuration Explanation
VLAN3	Port1 of PE1 and PE2
dot1q-tunnel	Port1 of PE1 and PE2
tpid	Port10 of PE1
Trunk port	Port10 of PE1 and PE2

Configuration procedure is as follows

PE1

SS2R48G4I (Config)#vlan 3
SS2R48G4I (Config-Vlan3)#switchport interface ethernet 0/0/1
SS2R48G4I (Config-Vlan3)#exit
SS2R48G4I (Config)#dot1q-tunnel enable
SS2R48G4I (Config)#dot1q-tunnel tpid 9100
SS2R48G4I (Config)#interface ethernet 0/0/1
SS2R48G4I (Config-Ethernet0/0/1)#switchport dot1q-tunnel mode customer
SS2R48G4I (Config-Ethernet0/0/1)#exit
SS2R48G4I (Config)#interface ethernet 0/0/10
SS2R48G4I (Config-Ethernet0/0/10)#switchport mode trunk
SS2R48G4I (Config-Ethernet0/0/10)#switchport dot1q-tunnel mode uplink
SS2R48G4I (Config-Ethernet0/0/10)#exit
SS2R48G4I (Config)#

PE2

SS2R48G4I (Config)#vlan 3

```
SS2R48G4I (Config-Vlan3)#switchport interface ethernet 0/0/1
SS2R48G4I (Config-Vlan3)#exit
SS2R48G4I (Config)#dot1q-tunnel enable
SS2R48G4I (Config)#interface ethernet 0/0/1
SS2R48G4I (Config-Ethernet0/0/1)#switchport dot1q-tunnel mode customer
SS2R48G4I (Config-Ethernet0/0/1)#exit
SS2R48G4I (Config)#interface ethernet 0/0/10
SS2R48G4I (Config-Ethernet0/0/10)#switchport mode trunk
SS2R48G4I (Config-Ethernet0/0/10)#switchport dot1q-tunnel mode uplink
SS2R48G4I (Config-Ethernet0/0/10)#exit
SS2R48G4I (Config)#
```

9.3.4 Dot1q-tunnel Troubleshooting

- This function cannot be used simultaneously with private-vlan(refer to session 9.2.2.9).
- customer port mode has to be configured on access ports, while the uplink port mode has to be configured on trunk ports.
- It is recommened that using the uplink pord mode on 1000bps ports to reach the expected transimission rate of uplink ports and guarantee the high-speed operation of network.

9.4 Protocol VLAN Configuration

9.4.1 Protocol VLAN Introduction

To be simple and clear, Protocol VLAN mirrors packets without tags to VLAN according to their protocol types, instead of determining their VLAN identity according to the physical ports of the switches they connect to. After configureing the Protocol VLAN, the switch will check the packets received on the ports, designating a VLAN membership to them based on their protocol types and encapsulation types. For example, after configuring the IPV4 protocol VLAN encapsulated by ehternet II, when receiving a packet of this kind without a VLAN tag, it will be classified as a member of the VLAN specified by IP protocol.

Protocol VLAN filter is only applied to the received packets without a VLAN tag. The packets with VLAN tags received on the same port will not be affected and will keep their original state.

Protocol VLANs do not create new VLAN, but share with port-based VLANs. Once the packets enters these VLANs, they will be transimitted according to the same rules as port-based VLANs use.

Classified by network layer protocols, different protocols can belongs to different VLANs. This is very attractive for those networks hoping to organize users aiming at specific applications and services. Beside, users can move as they will within the network while keeping their VLAN membership unchanged. The advantage of this method is that, the physical location of users can change without reconfigureing the VLAN they belong to. And it is also very significant for the network managers that the VLAN can be classified by protocol type. What's more, this method does not need additional frame tag to identify VLANs,and thus can decrease the communication traffic of the network.

In SS2R24/48G4i switch, 1000bps network ports can support Protocol VLAN fucntion unconditionally, while the 100bps wthernet ports have to be set tgo trunk ports to use the function.

9.4.2 Protocol VLAN Configuration Task Sequence

1. Enable Protocol VLAN
2. Configure the protocol list entries

1. Enable Protocol VLAN

Command	**Explanation**
Global configuration mode	
protocol-vlan enable **no protocol-vlan enable**	Enable/disable Protocol VLAN

2. Configure the protocol list entries

Command	**Explanation**
Global configuration mode	
protocol-vlan mode {ethernetii etype <*etype-id*>|llc {dsap <*dasp-id*> ssap <*ssap-id*>}|snap etype <*etype-id*>} vlan <*vlan-id*> [priority <*priotiry-id*>] **no protocol-vlan {mode {ethernetii etype <*etype-id*>|llc {dsap <*dasp-id*> ssap <*ssap-id*>}|snap etype <*etype-id*>}|all}**	Add/delete the corresponding relationship between the protocol and VLAN, that is the specified protocol join/quilt the specified VLAN.

9.4.3 Protocol VLAN Troubleshooting

☞ Although there is no need, each IP protocol VLAN should contain an ARP protocol type, If not, the potential ARP failure might cause the diability to communicate

9.5 VLAN Troubleshooting

9.5.1 Monitor and Debug Comman

9.5.1.1 show vlan

Command show vlan [brief|private-vlan] [id <*vlan-id*>] [name <vlan-name>] [summary]
Function Display detailed information for all VLANs or specified VLAN.
Parameter **brief** stands for brief information; **summary** for VLAN statistics; **<*vlan-id*>** for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094; **<*vlan-name*>** is the VLAN name

for the VLAN to display status information, valid length is 1 to 11 characters.

Command mode Admin Mode

Displayed information	Explanation
VLAN	VLAN number
Name	VLAN name
Type	VLAN type, statically configured or dynamically learned
Status	Active, Status of VLAN
Ports	Access port within a VLAN

Chapter 10 RSTP CONFIGURATION

10.1 INTRODUCTION TO RSTP

RSTP is the abbreviation of Rapid Spanning Tree Protocol, which may block the redundant paths in exchanging network through rapid spanning tree algorithm and establish non-loop tree network. The rapid spanning tree algorithm adopted by RSTP is a distributed algorithm. It operates on all bridges of a Bridged-LAN, and is responsible for calculating a simple and interconnected active topology. It adopts a bridge as root (root bridge) when conducting calculation. At the same time, it designates roles for all ports of all bridges.

RSTP algorithm is basically consistent with the STP algorithm defined in the standard of IEEE 802.1D. The only difference is that RSTP overcomes the shortcoming of STP algorithm – For changing the state of any port from blocking state to forwarding state, it is necessary for STP algorithm to go through 2*forward-delay time. According to the different roles of ports in topology structure, RSTP may realize instant or fast transferring from blocking state to forwarding state.

According to functions of ports in active topology, RSTP defines five port roles disabled port, root port, designated port as well as alternate port and backup port which are specified for realizing instant performance. Introduction to the functions of each port role in active topology is as follows

1. Disabled ports do not participate in the algorithm of RSTP;
2. The bridge where the root port is located is connected to Root Bridge. The path cost from the bridge to Root Bridge through root port is the lowest.
3. The designated port connects a LAN to Root Bridge through the bridge connected to the port.
4. The alternate port provides alternate path from the bridge to Root Bridge other than the path from root port to Root Bridge.
5. The backup ports provide the alternate path from LAN at bridge downstream (the direction opposite to root) to Root Bridge.

The root port and designated port are part of active topology. They may conduct address learning and normal data forwarding. The alternate port, backup port and disabled port are not part of active topology. They do not conduct address-learning data forwarding.

10.2 RSTP CONFIGURATION

10.2.1 RSTP CONFIGURATION TASK SEQUENCE

1. startup **RSTP** and configure running mode

Command	**Explanation**
Global configuration mode and Port configuration mode	
spanning-tree **no spanning-tree**	Startup RSTP,the "**no spanning-tree"** command close RSTP function.
Global mode	
spanning-tree mode {rstp|stp} **no spanning-tree mode**	configure RSTP running mode,the "**no spanning-tree mode**" command restores default configuration
Port mode	
spanning-tree mcheck	Force port running in RSTP mode

2. Control **RSTP** elected active topology

Command	**Explanation**
global configuration mode	
spanning-tree priority *<bridge-priority>* **no spanning-tree priority**	Configure switch priority,the " **no spanning-tree priority**" command restores default configuration
Port mode	
spanning-tree cost *<cost>* **no spanning-tree cost**	Configure Ethernet port path cost,the " **no spanning-tree cost**" command restores default configuration
spanning-tree port-priority *<port-priority>* **no spanning-tree port-priority**	Configure port priority, the " **no spanning-tree port-priority**" command restores default configuration

3. Configure **RSTP** network diameter and time Parameter

Command	**Explanation**
Global configuration mode	
spanning-tree diameter *<net-diameter>* **no spanning-tree diameter**	Configure switching network caliber,the " **no spanning-tree diameter**" command restores default configuration

spanning-tree forward-time <*time*> **no spanning-tree forward-time**	Configure switch forward time,the" **no spanning-tree forward-time**" restores default configuration
spanning-tree hello-time <*time*> **no spanning-tree hello-time**	Configure switch Hello time,the **"no spanning-tree hello-time"** command restores default configuration
spanning-tree maxage <*time*> **no spanning-tree maxage**	Configure switch maximum aging time,the " **no spanning-tree maxage**" command restores default configuration

4. Configure **RSTP** fast migration characteristic

Command	**Explanation**
Port configuration mode	
spanning-tree link-type point-to-point {auto|force-true|force-false} **no spanning-tree link-type**	Set port link type,the " no spanning-tree link-type"command restores auto link type
spanning-tree portfast **no spanning-tree portfast**	Configure port as port fast port,the " **no spanning-tree portfast**"configure non port fast port

10.3 RSTP Configuration Examples

The connection between the SW1-SW6 switches is showed in the chart above. By default, all the switches run in RSTP mode, their bridge priority, port priority and port link cost are all set to default value(all the same).The following is the default configuration of the switches

Name of the bgidge	The MAC address of the bridge	The bridge prioirty	Port priority			Link cost		
			Port 0/0/1	Port 0/0/2	Port 0/0/3	Port 0/0/1	Port 0/0/2	Port 0/0/3
SW1	…00-00-01	32768	128	128		200000	200000	
SW2	…00-00-02	32768	128	128		200000	200000	
SW3	…00-00-03	32768	128	128		200000	200000	
SW4	…00-00-04	32768	128	128	128	200000	200000	200000
SW5	…00-00-05	32768	128	128		200000	200000	
SW6	…00-00-06	32768	128	128		200000	200000	

By default, RSTP will automatically create a tree topology taking SWI as its root bridge(the port connected to the blue line is the forwarding port, while the one connected to the black line is discard).
Configuration Change

- Changing the bridge priority of switch 4 to 4096 will make the SW4 the root bridge;
- Changing the lick cost of the port 0/0/2 of switch 2 to 500000 will make port 0/0/1become the root port of SW2;
- The cost to reach root bridge from the port 0/0/1 of switch 3 shoudl be less than that from the port 0/0/1 of switch2, so the port 0/0/1 of switch 3 will be the specified port;

- Elevating the port priority of the port 0/0/1 of switch 4 to 160 while that of the port 0/0/3 of switch 4 is still the defaulted 128, will make the port 0/0/2 of switch 5 be the root port.

Name of the bgidge	**The MAC address of the bridge**	**The bridge prioirty**	**Port priority**			**Link cost**		
			Port 0/0/1	Port 0/0/2	Port 0/0/3	Port 0/0/1	Port 0/0/2	Port 00/3
SW1	…00-00-01	32768	128	128		200000	200000	
SW2	…00-00-02	32768	128	128		200000	500000	
SW3	…00-00-03	32768	128	128		200000	200000	
SW4	…00-00-04	4096	160	128	128	200000	200000	200000
SW5	…00-00-05	32768	128	128		200000	200000	
SW6	…00-00-06	32768	128	128		200000	200000	

Configuration procedure is as follows

Switch 4

Switch4#config↵

Switch4(Config)#spanning-tree↵

Switch4(Config)#spanning-tree priority 4096↵

Switch4(Config)#interface ethernet 0/0/1↵

Switch4(Config-Ethernet0/0/1)#spanning-tree port-priority 160↵

Switch 2

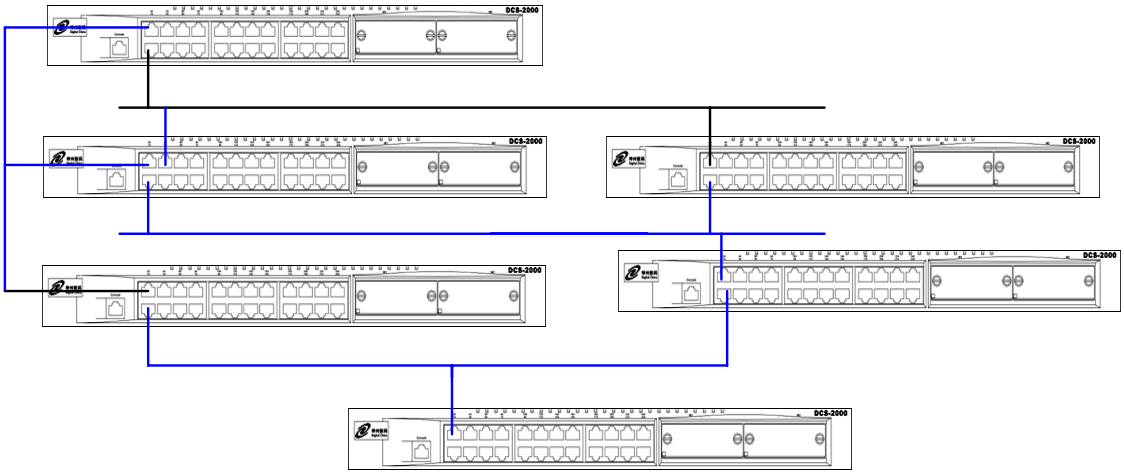
Switch2#config↵

Switch2 (Config)#spanning-tree

Switch2 (Config)#interface ethernet 0/0/2

Switch2 (Config-Ethernet0/0/2)#spanning-tree cost 500000

RSTP count result



10.4 RSTP Troubleshooting

10.4.1 Monitor and Debug Command

10.4.1.1 show spanning-tree

Command show spanning-tree [interface <*interface-list*>] [detail]
Function to display RSTP protocol information
Parameter <*interface-list*>is the port list; **[detail]** display detailed RSTP status of each port
Command mode Admin mode

Display Content	Explanation
STP version	STP version
Bridge Id Information	Switch information
Priority	Switch priority
Mac address	Switch MAC address
Bridge Max Age	Switch maxage time
Bridge Hello Time	Switch Hello time
Bridge Forward Delay	Switch forward delay
Bridge Diameter	Network diameter
Root bridge information	Root bridge information
Priority	Root bridge priority
Mac address	Root bridge MAC address
Root Path Cost	Switch root path cost
Root Port	Switch root port
Topology Changes	Topology changes
Current port list	Current port list in switch
Port	Port number
Priority	Port STP priority
Cost	Port cost
STPStatus	Port STP running status
PortState	Port status
Role	Port role
DesignatedBridge	Specified bridge ID(priority MAC address)
DsgPort	Specified port id

10.4.1.2 debug stp

Command debug stp {all | basic | in | out}

no debug stp {all|basic | in | out}

Function to open RSTP debug information. Use the "**no debug stp {all | basic | in | out}**" command to close RSTP debug information.

Parameter "**all"** means all debug information switch; **basic** table express as basic debug information switch; fsm table express as the limited status debug switch; **in** and **out** respective express as the debug switch of input packet and output packet。

Command mode Admin mode

10.4.2 RSTP TROUBLESHOOTING

- Users must turn on the RSTP switch in global mode before running RSTP in switch; otherwise user will not be able to turn on the port RSTP switch.
- There is correlation among parameters of RSTP timer. The switch will not function normally under incorrect configuration. The correlation between each timer is 2 X(Bridge_Forward_Delay-1.0 second) >= Bridge_Max_Age

Bridge_Max_Age >= 2 X(Bridge_Hello_Time + 1.0 second)

- Users should avoid unnecessary configuration of RSTP parameters only if they clearly understand the results that may cause.
- Users are not able to startup the port RSTP function with port MAC binding, 802.1x, and configuring the route port because it is manually exclusive with those three functions.

Chapter 11 IGMP Snooping

11.1 Introduction to IGMP Snooping

IGMP (Internet Group Management Protocol) is a protocol used in IP multicast. IGMP is used by multicast enabled network device (such as a router) for host membership query, and by hosts that are joining a multicast group to inform the router to accept packets of a certain multicast address. All those operations are done through IGMP message exchange. The router will use a multicast address (224.0.0.1) that can address to all hosts to send a IGMP host membership query message. If a host wants to join a multicast group, it will reply to the multicast address of that a multicast group with a IGMP host membership reports a message.

IGMP Snooping is also referred to as IGMP listening. The switch prevents multicast traffic from flooding through IGMP Snooping, multicast traffic is forwarded to ports associated to multicast devices only. The switch listens to the IGMP messages between the multicast router and hosts, and maintains multicast group forwarding table based on the listening result, and can then decide to forward multicast packets according to the forwarding table.

SS2R24/48G4i switch switch provides IGMP Snooping and is able to send a query from the switch so that the user can use SS2R24/48G4i switch switch in IP multicast.

11.2 IGMP Snooping Configuration

11.2.1 IGMP Snooping Configuration Task

1. Enable IGMP Snooping
2. Configure IGMP Snooping

1.Start IGMP Snooping function

Command	**Explanation**
Global configuration mode	
Ip igmp snooping **No ip igmp snooping**	Start IGMP Snooping function;the ” No ip igmp snooping” command will shut down the IGMP snooping function globally.

2. Configure IGMP Snooping

Command	**Explanation**
Global configuration mode	
Ip igmp snooping vlan <*vlan-id*> **No ip igmp snooping vlan <*vlan-id*>**	Start IGMP Snooping function on the specified vlan.” No ip igmp snooping vlan <vlan-id> “ command will disalbe IGMP function on the sepcified vlan.
Ip igmp snooping vlan < *vlan-id* > limit	Set the max number of the groups IGMP

{group <*g_limit*> | source <*s_limit*>} **No ip igmp snooping vlan < *vlan-id* > limit**	snooping can join and the max number of sources each group can have." No ip igmp snooping vlan < vlan-id > limit " will reset it to default value.
Ip igmp snooping vlan <*vlan-id*> l2-general-querier **No ip igmp snooping vlan <*vlan-id*> l2-general-querier**	Set this vlan to a layer 2 general queirer. It is recommended that each segment should configure a layer 2 general queirer." No ip igmp snooping vlan <vlan-id> l2-general-querier" command will cancel the configuration of layer 2 general queirer
Ip igmp snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*> **No ip igmp snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*>**	Set the static mrouter por." No ip igmp snooping vlan <vlan-id> mrouter-port interface <interface –name>"command will cancel the configuration of mrouter port.
Ip igmp snooping vlan <*vlan-id*> mrpt < *value* > **No ip igmp snooping vlan <*vlan-id*> mrpt**	Set the keep-alive time of the mrouter port, the" No ip igmp snooping vlan <vlan-id> mrpt" command will reset it to default value
Ip igmp snooping vlan <*vlan-id*> query-interval <*value*> **No ip igmp snooping vlan <*vlan-id*> query-interval**	Set the query interval, "No ip igmp snooping vlan <vlan-id> query-interval " command will reset it to default value.
Ip igmp snooping vlan <*vlan-id*> immediate-leave **No ip igmp snooping vlan <*vlan-id*> immediate-leave**	Set the IGMP snooping of specified vlan to enable the immediate-leave function;" No ip igmp snooping vlan <vlan-id> immediate-leave"command will cancel immediate-leave configuraiton.
Ip igmp snooping vlan <*vlan-id*> query-mrsp <*value*> **No ip igmp snooping vlan <*vlan-id*> query-mrsp**	Set the max query response time," No ip igmp snooping vlan <vlan-id> query-mrsp" command command will reset it to default value.
Ip igmp snooping vlan <vlan-id> query-robustness <*value*> **No ip igmp snooping vlan <vlan-id> query-robustness**	Set the robustness, "No ip igmp snooping vlan <vlan-id> query-robustness" will reset it to default value.
Ip igmp snooping vlan <*vlan-id*> suppression-query-time <*value*> **No ip igmp snooping vlan <*vlan-id*> suppression-query-time**	Set the suppression time of query; "No ip igmp snooping vlan <vlan-id> suppression-query-time" will reset it to default value.
ip igmp snooping vlan <*vlan-id*> tatic-group <multicast-IPAddress> interface {[ethernet|port-channel] <interfaceName> **No ip igmp snooping vlan <*vlan-id*>**	Set the statci group of the specified port, the "No ip igmp snooping vlan <vlan-id> tatic-group <multicast-IPAddress> interface {[ethernet|port-channel] <interfaceName> command will cancel the configuration.

tatic-group <multicast-IPAddress> interface {[ethernet|port-channel] <interfaceName>	

11.3 IGMP Snooping Examples

Scenario 1 IGMP Snooping function

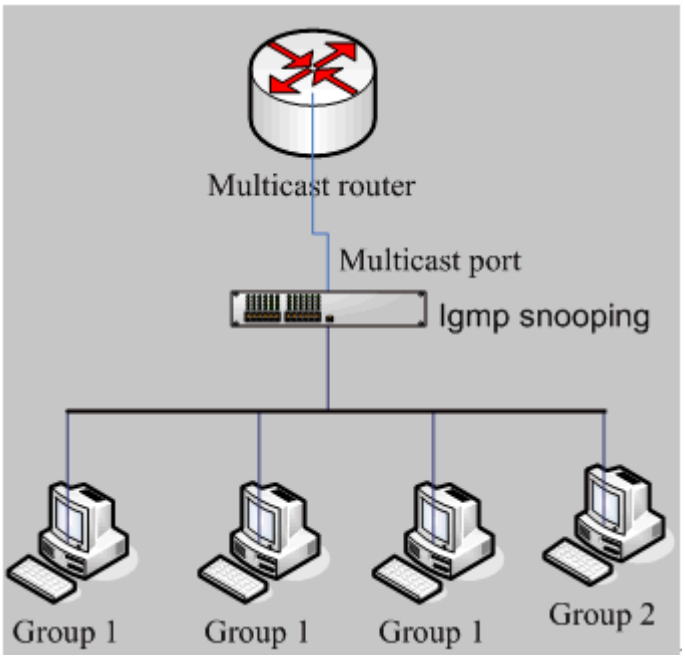


Fig 11-1 Enabling IGMP Snooping function

Example As shown in the above figure, a VLAN 100 is configured in the switch and includes ports 1, 2, 6, 10 and 12. Four hosts are connected to port 2, 6, 10, 12 respectively and the multicast router is connected to port 1. As IGMP Snooping is disabled by default either in the switch or in the VLANs, If IGMP Snooping should be enabled in VLAN 100, the IGMP Snooping should be first enabled for the switch in Global Mode and in VLAN 100 and set port 1 of VLAN 100 to be the M-Router port.
The configuration steps are listed below
switch#config
switch (config)#ip igmp snooping
switch (config)#ip igmp snooping vlan 100
switch (config)#ip igmp snooping vlan 100 mrouter-port interface ethernet 0/0/1

Multicast Configuation
Assuming that there are two multicast servers Multicast Server 1and Multicase Server 2. Multicast Server 1 provides program1 and program 2 while the Multicast Server 2 provides program3. And they use group addresses Group1，Group2 and Group 3 respectively. There are four hosts running multicast application software simultaneously, the two of which connected to port 2 and 6 order program 1, the

one connected to port 10 orders program2 and the other one connected to port 12 orders program 3
IGMP Snooping listening result
The multicast table built by IGMP Snooping in VLAN 100 indicates ports 1, 2, 6, 10 in Group1 and ports 1, 12 in Group3.
All the four hosts can receive the program of their choice ports 2, 6, 10 will not receive the traffic of program 2,3and port 12 will not receive the traffic of program 1,2.

Scenario 2 IGMP L2-general-querier

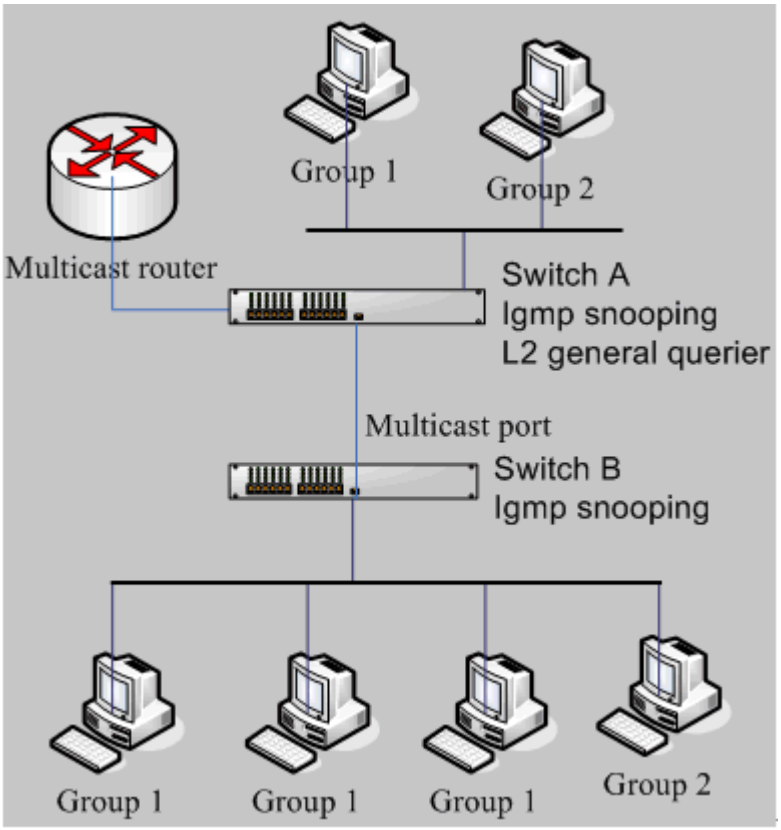


Fig 11-2 The switches as IGMP Queries

The configuration of Switch2 is the same as the switch in scenario 1, SwitchA takes the place of Multicast Router in scenario 1. Let's assume VLAN 60 is configured in SwitchA, including ports 1, 2, 6, 10 and 12. Port 1 connects to the multicast server, and port 2 connects to Switch2. In order to send Query at regular interval, IGMP query must enabled in Global mode and in VLAN60.

The configuration steps are listed below

switchA#config
switchA(config)#ip igmp snooping
switchA(config)#ip igmp snooping vlan 60
switchA(config)#ip igmp snooping vlan 60 l2-general-querier

switchB#config
switchB(config)#ip igmp snooping
switchB(config)#ip igmp snooping vlan 100
switchB(config)#ip igmp snooping vlan 100 mrouter interface ethernet 0/0/1

Multicast Configuration
The same as scenario 1.
IGMP Snooping listening result
Similar to scenario 1.

11.4 IGMP SnoopingIGMP Snooping Troubleshooting

11.4.1 IGMP Snooping Monitor and Debug Command

11.4.1.1 debug igmp snooping all/packet/event/timer/mfc

Command debug igmp snooping all/packet/event/timer/mfc
no debug igmp snooping all/packet/event/timer/mfc
Function Enable the IGMP Snooping debug swithc of the switch; the “no debug igmp snooping all/packet/event/timer/mfc” command is to disable the debug switch.
Command Mode Admin Mode
Default Setting By default the IGMP Snooping debug seitch of the switch is disabled.

11.4.1.2 show ip igmp snooping

Command show ip igmp snooping [vlan <*vlan-id*>]
Parameter **<*vlan-id*>** is vlan number of specify display IGMP Snooping information
Command Mode Admin mode
1. Display the summary infromation of IGMP Snooping of the switch

Displayed Informaton	Explanation
Global igmp snooping status	Whether the global igmp snooping switch of the swithc is enabled.
Igmp snooping is turned on for vlan 1(querier)	Which vlans of the switch enable igmp snooping function, and whether they are l2-general-queriers

2..Display the detailed information of IGMP Snooping of vlan1

Displayed Informaton	Explanation
Igmp snooping L2 general querier	Whether vlan has started l2-general-querier function; and display the state of the querier could-query or suppressed
Igmp snooping query-interval	The query interval of the vlan
Igmp snooping max reponse time	The max reponse time of the vlan
Igmp snooping robustness	The robustness of the vlan

Igmp snooping mrouter port keep-alive time	The keep-alive time vlan of the vlan
Igmp snooping query-suppression time	The query-suppression time of the vlan as a l2-general-querier
IGMP Snooping Connect Group Membership	The group membership of the vlan，that is the corresponding relationship between the port and(S,G).
Igmp snooping vlan 1 mrouter port	The mrouter port of the vlan, including static and dynamic.

11.4.1.3 show mac-address-table multicast

Command show mac-address-table multicast
Function Show the multicast MAC address table messages
Parameter None
Command Mode Admin Mode
Default Not showing the multicast MAC address and port mapping by system default

11.4.2 IGMP Snooping Troubleshooting

When configuring and using IGMP Snooping function, users might find that the IGMP Snooping work abnormally, probablely because of the reasons like incorrect physical connection and configuration. So, the user should ensure the following

- Guarantee that the physical connection is corretct;
- Ensure that the IGMP Snooping is enabled in global configuration mode(using ip igmp snooping); ;
- Ensure that vlan has configured with IGMP Snooping in global configuration mode(using ip igmp snooping vlan <vlan-id>);
- Ensure that a vlan is configured as a layer 2 general queirer or a static mrouter is configured in the same segment.
- Check the validityof IGMP Snooping information usingcommand”show ip igmp snooping vlan <vid>”.

If all the above ways cannot solve the problems of IGMP Snooping, please use debug commands like” debug igmp snooping” , then copy the DEBUG information in 3miniutes and send the information to the technical service center of our company.

Chapter 12 Multicast VLAN Configuration

12.1 Multicast VLAN Introduction

Based on the current multicast programordering method, when users in different VLANs order programs, each VLAN will copy a multicast stream within itself. This method will waste lots of bandwidth. So by configuring multicast VLAN, we add the ports of a switch to a multicast VLAN, after enabling the IGMP Snooping function, we can make users in different VLANs share a same multicast VLAN, and limit the transimisstion of multicast stream within only one multicast VLAN. Thus, bandwidth will be saved. Since the multicast VLAN and user VLAN are completely isolated, both the security and the bandwidth can be guaranteed. After we configure the multicast VLAN, we can ensure that the multicast information stream can be sent to users without a stop.

12.2 Multicast VLAN Configuration

12.2.1 Multicast VLAN Configuration Task Sequence

1.Start multicast VLAN function
2.Configure IGMP Snooping

1. Start multicast VLAN function

Command	**Explanation**
VLAN configuration modeg	
multicast-vlan **no multicast-vlan**	Configure a VLAN to start the multicast VLAN function. The ” no multicast-vlan” command will disable the multicast VLAN function of the VLAN.
multicast-vlan association <*vlan-list*> **no multicast-vlan association <*vlan-list*>**	Associate a multicst VLAN to other VLANs. The ” no multicast-vlan association <vlan-list>” command will delete the accosiated VLANs of the multicast VLAN.

2.Configure IGMP Snooping

Command	**Explanation**
Global configuration mode	
ip igmp snooping vlan <*vlan-id*> **no ip igmp snooping vlan <*vlan-id*>**	Start the IGMP Snooping function of the multicast vlan. “no ip igmp snooping vlan <vlan-id>” command will disable the IGMP Snooping function of the multicast vlan.
ip igmp snooping **no ip igmp snooping**	Start the IGMP Snooping function. The “no ip igmp snooping ” command will disable

	the IGMP Snooping function globally.

12.3 Multicast VLAN Examples

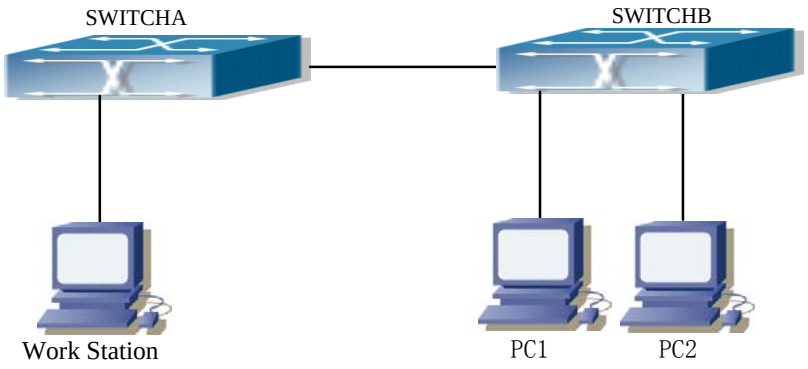


Fig 2-12-1 The function configuration of multicast VLAN

As showed in the picture above, multicast server connects to a 3-layer switch switchA via port 0/0/1,and the port 0/0/1 belongs to the vlan10 of the switch. 3-lay switch switchA connects to 2-layer switch switchB via port . Vlan 20 is a multicast vlan. The vlan 100 of switchB includes port 0/0/15，vlan101 includes port 0/0/20. PC1 and PC2 connect to port 0/0/15 and respectively. switchB connects to switchA via port . Vlan20 is a multicast vlan.

By configuring multicast VLAN, we can make PC1 and PC2 to receive multicast data viamulticast VLAN.

The following configuration is based on the assupmtion that the IP address of switchA has been configured, and the devices are connected correctly.

The following is the configuration procedure

```
switchA#config
switchA (config)#vlan 10
switchA (config-vlan10)#switchport access ethernet
switchA (config-vlan10)exit
switchA (config)#interface vlan 10
switchA(Config-if-Vlan10)#ip pim dense-mode
switchA(Config-if-Vlan10)#exit
switchA (config)#vlan 20
switchA (config-vlan20)#multicast-vlan
switchA (config-vlan20)#exit
switchA (config)#ip igmp snooping
switchA (config)#ip igmp snooping vlan 20
switchA (config)#interface vlan 20
switchA(Config-if-Vlan20)#ip pim dense-mode
switchA(Config-if-Vlan20)#exit
switchA (config)#ip pim multicast
```

switchA (config)# interface ethernet
switchA (Config-Ethernet)switchport mode trunk

switchB#config
switchB (config)#vlan 100
switchB (config-vlan100)#switchport access ethernet
switchB (config-vlan100)exit
switchB#config
switchB (config)#vlan 101
switchB (config-vlan101)#switchport access ethernet
switchB (config-vlan101)exit
switchB (config)# interface ethernet
switchB (Config-Ethernet)#switchport mode trunk
switchB (Config-Ethernet)#exit
switchB (config)#vlan 20
switchB (config-vlan20)#multicast-vlan
switchB (config-vlan20)#multicast-vlan association 100,101
switchB (config-vlan20)#exit
switchB (config)#ip igmp snooping
switchB (config)#ip igmp snooping vlan 20

Chapter 13 DCSCM Configuraion

13.1 DCSCM Introduction

DCSCM(security control multicast)technology includes three respects multicast source controllabillity, multicast users controllabillity and the service-priority-oriented multicast policy.

The DCSCM technology mainly use the following methods to realize multicast source controllabillity

a) On the boundary switch, if configured the source-controlled multicast, only the muticast data of the specified group sent by specified source can pass.

b) For the RP switch at the PIM-SM core state, REGISTER_STOP will be directly sent for all the REGISTER information besides than the specified source and group.Creating list entries is not allowed.(This task is implemented in PIM-SM module).

The implementation of DCSCM technology is based on the contro lboer the IGMP report messages from users, so the controlling modules are IGMP snooping module and IGMP module. The control logic of it includes the following three methods control according to the source VLAN+MAC address of the message, control according to the source IP address of the message, and control according to the port through which the message enters.IGMP snooping can use all the three methods while the IGMP, since it is at layer 3, can only control according to the source IP address of the messgae.

The service-priority-oriented mutilcast policy of DCSCM technology adpots the following methods for the multicast data within a limited range, the user-specified priority is set at the access point, making data be transmitted on TRUNK at a higher priority, and thus ensuring the data to be transmitted through the whole network at the user-specified priority.

13.2 DCSCM Configuration

13.2.1 DCSCM Configuration Task Sequence

（1） Configuration of source control

（2） Configuration of destination control

（3） Configuration of multicast policy.

1. Configuration of source control

Configuration of source control can be divided into three parts, the first is to enable the source control globally, the following is th command to do this

Command	Explantation
Global configuration mode	

[no] ip multicast source-control(necessary)	Enable the source control globally, the “[no] ip multicast source-control” command will disable the source control globally. What calls for attention is that after the global source control is enabled, all the multicast messages will be dumped by default. All the souce control configuration can only be done after it is enabled globally, and only when all the configured rules has been disabled, can the souce control be disabled globally.

The next is the configuration of the rules of source control. It adopts the same method adopted by ACL, using ACL ID from 5000 to 5099 的 ACL, each rule ID can configure 10 rules at most. What calls for attention is that, these rules has a sequence, the rule configured earliest is at the front, once it is matched, all the following rules will be neglected. So the rules that are allowed globally should be configured as the last rule. The following is the command to do this

Command	**Explantation**
Global configuration mode	
[no] access-list *<5000-5099>* {deny|permit} ip {{*<source>* *<source-wildcard>*}|{host-source *<source-host-ip>*}|any-source} {{*<destination>* *<destination-wildcard>*}|{host-destination *<destination-host-ip>*}|any-destination}	To configure the rules used in source control. The rule can only take effect on specified port. Prefixing the command with “NO” will delete the specified rule.

Attention since the configured rules take up the list entries of hardware, too many rules might cause the configuration to fail because the underlying list entries are full. So we recommend that users should use rules as simple as possible.The following is the command to configure.

Command	**Explantation**
Port configuration mode	
[no] ip multicast source-control access-group *<5000-5099>*	To configure the rule used in source control to a port, prefixing the command with “NO” will cancel the configuration.

2. Configuration of destination control

Similar to the configuration of source control, it has three steps

The first step is to globally enable destination control, since the destination control should prevent the unauthorized users to receive the multicast data, after the global destination control, the switch will not broadcast the multicast data it receives. So, we should avoid to connect two or more other 3-layer switches to a switch with destination control enabled within one VLAN.The following is the command to configure

Command	Explantation
Global configuration mode	
[no] ip multicast destination-control(necessary)	Enable the destination globally. The" no ip multicast destination-contro" command will disable the destination control globally.Only after the desination control is enabled globally, all of the other configurations can take effect.

The next step is to configure the destination control rules, which is also similar to that ofsource control except that it uses ACL ID from 6000 to 7999.

Command	Explantation
Global configuration mode	
[no] access-list *<6000-7999>* {deny|permit} ip {{*<source>* *<source-wildcard>*}|{host-source *<source-host-ip>*}|any-source} {{*<destination>* *<destination-wildcard>*}|{host-destination *<destination-host-ip>*}|any-destination}	Configure the rule used in destination control. The rule can only take effect when applied to specified source IP or VLAN-MAC and port. Prefixing the command with "NO" can delete the specified rule.

The last step is to configure the rule to specified source IP, source VLAN MAC or port.What calls for attention is that, taking the above statement, only after enabling IGMP-SNOOPING can we use the rules globally, if not, only source IP rules can be used in IGMP protocol. If we configure source IP,VLAN MAC and specified port rules, the rules are matched to messages in a sequence as VLAN MAC, sourve IP, specified ports. The folloing is the command to configure

Command	Explantation
Port configuration mode	
[no] ip multicast destination-control access-group *<6000-7999>*	To configure the rule used in source control to a port, prefixing the command with "NO" will cancel the configuration.
Global configuration mode	
[no] ip multicast destination-control *<1-4094>* *<macaddr>* access-group *<6000-7999>*	To configure the rule used in source control to specified VLAN-MAC, prefixing the command with "NO" will cancel the configuration.

[no] ip multicast destination-control *<source>* *<source-wildcard>* access-group *<6000-7999>*	To configure the rule used in source control to specified source IP address/MASK, prefixing the command with “NO” will cancel the configuration.

3. Configuration of mulicast policy

mulicast policy satisfies the demand of special users by designating priority for specified multicast data. What calls for attention is that multicast data can only be taken special care when it is transmitted on TRUNK . The following is the command to configure(set a priority for the specified multgicast)

Command	**Explantation**
Global configuration mode	
[no] ip multicast policy *<source>* *<source-wildcard>* *<destination>* *<destination-wildcard>* cos *<priority>*	Configure the multicast policy, set priority for source within a special range. The range of priority is <0-7>.

13.3 DCSCM Typical Examples

1. Souce control

To prevent a boundary switch to send multicast data freely, we configure on the boundary switch that, only the switch connected to port Ethernet0/0/5 is allowed to send multicast data, and the group of the data has to be 225.1.2.3. But the uplink port Ethernet0/0/25 can forward multicast data without limitation. The following is the configuration we can make

Switch(Config)#access-list 5000 permit ip any host 225.1.2.3
Switch(Config)#access-list 5001 permit ip any any
Switch(Config)#ip multicast source-control
Switch(Config)#interface Ethernet0/0/5
Switch(Config-If-Ethernet0/0/5)#ip multicast source-control access-group 5000
Switch(Config)#interface Ethernet0/0/25
Switch(Config-If-Ethernet0/0/25)#ip multicast source-control access-group 5001

Destination control

We can confiure as follows if we want to prevent the users in 10.0.0.0/8 segment to join the group 238.0.0.0/8

Firstly, to enable IGMP snooping in the VLAN it is in(assumed to be VLAN2)
Switch(Config)#ip igmp snooping
Switch(Config)#ip igmp snooping vlan 2
Then, configure the relative detination control ACL, and configure the specified IP to use the ACL.
Switch(Config)#access-list 6000 deny ip any 238.0.0.0 0.255.255.255
Switch(Config)#access-list 6000 permit ip any any
Switch(Config)#ip multicast destination-control
Switch(Config)#ip multicast destination-control 10.0.0.0 0.255.255.255 access-group 6000

Thus, the users of this segment can only join the groups other than 238.0.0.0/8

3. Multicast policy

Server 210.1.1.1 is sending important multicast data in the group 239.1.2.3 上, we can configure as follows on its access switch

Switch(Config)#ip multicast policy 210.1.1.1 0.0.0.0 239.1.2.3 0.0.0.0 cos 4

Thus when the multicast strem is passing the TRUNK of this switch to other switches, it will be at priority 4(usually it is a high priority, the higher might be protocol data, but if we set higher priority, when there is too much multicast data, may cause abnormal behavior of the switch protocol)

13.4 DCSCM Troubleshooting

13.4.1 DCSCM Debug and Monitor Command

13.4.1.1 show ip multicast source-control access-list

Command **show ip multicast source-control access-list**
show ip multicast source-control access-list <5000-5099>
Function To display the configured source control multicast ACL.
Parameters ***<5000-5099>*** **ACL ID**
Default Settings None.
Command Mode Admin Mode

13.4.1.2 show ip multicast destination-control access-list

Command **show ip multicast destination-control access-list**
show ip multicast destination-control access-list <*6000-7999*>
Function To display the configured destination control multicast ACL,
Parameters *<6000-7999>* ACL ID.
Default Settings None.
Command Mode Admin Mode

13.4.1.3 show ip multicast policy

Command **show ip multicast policy**
Function To display the configured multicast policy.
Parameters None.
Default Settings None.
Command Mode Admin Mode

13.4.1.4 show ip multicast source-control

Command **show ip multicast source-control [detail]**
show ip multicast source-control interface <Interfacename> [detail]
Function To display the multicst control configuration.

Parameters **detail** whether display detailed information.

<Interfacename> interface name，like Ethernet 0/0/1or ethernet 0/0/1。

Default Settings None.

Command Mode Admin Mode

13.4.1.5 show ip multicast destination-control

Command **show ip multicast destination-control [detail]**

show ip multicast destination-control interface <Interfacename> [detail]

show ip multicast destination-control host-address <ipaddress> [detail]

show ip multicast destination-control <vlan-id> <mac-address> [detail]

Function To display the multicast destination configuration

Parameters **detail** whether display detailed information.

<Interfacename> interface name，like Ethernet 0/0/1 or port-channel 1 or ethernet 0/0/1。

Default Settings None.

Command Mode Admin Mode

13.4.2 11.4.2 DCSCM Troubleshooting

DCSCM module has similar function with ACL, the problems usually relate with incorrect configuration. Please read the instruction above carefully. If you still cannot pin down the cause of the problems, please send your configuration and the error messages to our technical support contact support@amer.com.

Chapter 14 802.1x Configuration

14.1 Introduction to 802.1x

IEEE 802.1x is a port-based network access management method, which authenticates and manages the accessing devices on the physical access level of the LAN device. The physical access level here are the ports of the switch. If the users' devices connected to such ports can be authenticated, access to resources in the LAN is allowed; otherwise, access will be denied, which is essentially the same as disconnecting physically.

IEEE 802.1x defines a port-based network access management protocol. It should be noted that the protocol applies to point-to-point connection between the accessing device and the access port, where the port can be either a logical port or a physical port. Typically, one physical port of the switch connects with one terminal device (physical port-based) only.

The architecture of IEEE 802.1x is shown below

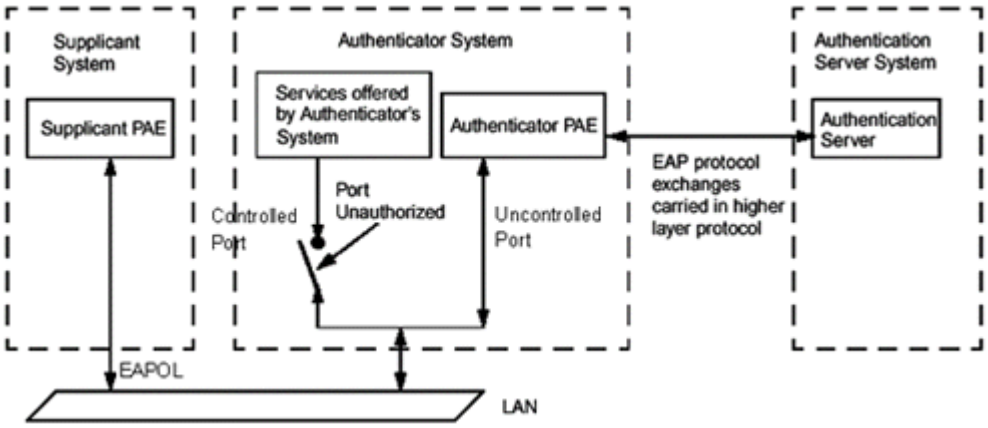


Fig 14-1 802.1x architecture

As shown in the above figure, the IEEE 802.1x architecture consists of three parts

- Supplicant System (user access devices)
- Authenticator System (access management unit)
- Authentication Server System (the authenticating server)

EAPOL protocol defined by IEEE 802.1x runs between the user access device (PC) and access management unit (access switch); and EAP protocol is also used between the access management unit and authenticating server. EAP packets encapsulates the authenticating data. The EAP packet is conveyed in the packets of the higher layer protocols such as RADIUS to pass through complex network to the authenticating server.

The ports provided by the port-based network access management device end are divided into two virtual port types managed port and non-managed port. A non-managed port is always in the connected status for both in and out directions to transfer EAP authenticating packets. A managed port will be in the connected status when authorized to transfer commutation packets; and is shutdown when not authorized, and cannot transfer any packets.

In the IEEE 802.1x application environment, SS2R24/48G4i switch is used as the access management unit, and the user connection device is the device with 802.1x client software. An authenticating server usually reside in the Carrier's AAA center and usually is a Radius server.

the difference between user access, MAC-based IEEE 802.1x authentication is implemented in SS2R24/48G4i switch for better security and management. Only authenticated user access devices connecting to the same physical port can access the network, the unauthorized devices will not be able to access the network. In this way, even if multiple terminals are connected via one physical port, SS2R24/48G4i switch can still authenticate and manage each user access device individually.

User-based (IP address+ MAC address+ port) 802.1x authentication function is implemented on the base of MAC-based 802.1x authentication function, allowing users to access restricted resources before being authenticated. For user-based access control mode, there are two modes standard control and advanced control. User-based standard control type does not limit the access to restricted resources, all the users of the port can access restricted resources before being authenticated, and after being authenticated, users can access all the resources; while the user-based advanced control will limit the access to restricted resources, only special users of the port can access restricted resorce before being authenticated,after passing the authentication, they can access all the resources.

14.2 802.1x Configuration

14.2.1 802.1x Configuration Task List

1.Enable IEEE 802.1x function
2.Access management unit property configuration
  1) Configure port authentication status
  2) Configure access management method for the port MAC-based or port-based.
  3) Configure expanded 802.1x function
3. User access devices related property configuration (optional)
4. RADIUS server related property configuration
  1) Configure RADIUS authentication key.
  2) Configure RADIUS Server
  3) Configure RADIUS Service parameters.

1. Enable 802.1x function	
Command	**Explanation**
Global Mode	
aaa enable no aaa enable	**Enables the AAA authentication function in the switch; the "no aaa enable" command disables the AAA authentication function.**
aaa-accounting enable no aaa-accounting enable	**Enables the accounting function in the switch; the "no aaa-accounting enable"**

	command disables the accounting function
aaa-accounting update {enable|disable}	**Enables/disables accounting update**
dot1x enable no dot1x enable	**Enables the 802.1x function in the switch and ports; the "no dot1x enable" command disables the 802.1x function.**
dot1x privateclient enable no dot1x privateclient enable	**Enable the switch to force the client software adopts AMER.COM private 802.1x authentication message format; the "no dot1x privateclient enable" command is used to disable this function, and thus allow the client software to adopt standard 802.1x authentication message format;**
dot1x user free-resource *<prefix>* *<mask>* no dot1x user free-resource	**Set the limited resources can be accessed by users;the "no dot1x user free-resource" command is used to delete the limited resources.**

2. Access management unit property configuration

1) Configure port authentication status

Command	Explanation
Global Mode	
dot1x port-control {auto|force-authorized|force-unauthorized|vlanstyle } **no dot1x port-control**	Configures 802.1x authorized status,the " **no dot1x port-control**" restore default configration

2) Configure port access management method

Command	Explanation
Global Mode	
dot1x port-method {macbased | portbased | userbased { standard | advanced}} **no dot1x port-method**	Sets the port access management method; the "no dot1x port-method" command restores MAC-based access management.
dot1x max-user macbased *<number>* **no dot1x max-user macbased**	Sets the maximum number of access users for the specified port; the "no dot1x max-user **macbased**" command restores the default setting of allowing 1 user.

dot1x max-user userbased <*number*> **no dot1x max-user userbased**	Set the max number of the users allowed to access by specified port, applied to ports using userbased access control mode; the " no dot1x max-user userbased " command is used to reset the default value allowing 10 users at most.

3) Configure expanded 802.1x function

Command	**Explanation**
Global Mode	
dot1x macfilter enable no dot1x macfilter enable	**Enables the 802.1x address filter function in the switch; the "no dot1x macfilter enable" command disables the 802.1x address filter function.**
dot1x accept-mac <mac-address> [interface <interface-name>] no dot1x accept-mac <mac-address> [interface <interface-name>]	**Adds 802.1x address filter table entry, the "no dot1x accept-mac" command deletes 802.1x filter address table entries.**
dot1x eapor enable no dot1x eapor enable	**Enables the EAP relay authentication function in the switch; the "no dot1x eapor enable" command sets EAP local end authentication.**
dot1x unicast enable no dot1x unicast enable	**Enable the 802.1x single-cast authentication function of the switch; the "no dot1x unicast enable" command is used to diable the802.1x single-cast authentication function.**
dot1x BPDU_forward enable no dot1x BPDU_forward enable	**Enable the 802.1x traversal function of the switch; the "no dot1x BPDU_forward enable " command is used to diable the 802.1x traversal function of the switch.**
dot1x freevlan <vlanID> no dot1x freevlan	**Set the 802.1x freevlan of the switch; the" no dot1x freevlan" command is used to disable the 802.1x freevlan function.**

3. Supplicant related property configuration

Command	Explanation
Global Mode	

dot1x max-req <*count*> **no dot1x max-req**	Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response, the “no dot1x max-req” command restores the default setting.
dot1x re-authentication **no dot1x re-authentication**	Enables periodical supplicant authentication; the “no dot1x re-authentication” command disables this function.
dot1x timeout quiet-period <*seconds*> **no dot1x timeout quiet-period**	Sets time to keep silent on port authentication failure; the “no dot1x timeout quiet-period” command restores the default value.
dot1x timeout re-authperiod <*seconds*> **no dot1x timeout re-authperiod**	Sets the supplicant re-authentication interval; the “no dot1x timeout re-authperiod” command restores the default setting.
dot1x timeout tx-period <*seconds*> **no dot1x timeout tx-period**	Sets the interval for the supplicant to re-transmit EAP request/identity frame; the “no dot1x timeout tx-period” command restores the default setting.
Admin Mode	
dot1x re-authenticate [interface <*interface-name*>]	Enables IEEE 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.

4. Authentication Server (RADIUS server) related property configuration

1) Configure RADIUS authentication key

Command	Explanation
Global Mode	
radius-server key **<*string*>** **no radius-server key**	Specifies the key for RADIUS server; the “no radius-server key” command deletes the key for RADIUS server.

2) Configuring RADIUS Server

Command	Explanation
Global Mode	
radius-server authentication host <*IPaddress*> [[port {<*portNum*>}] [primary]] **no radius-server authentication host <*IPaddress*>**	Specifies the IP address or IPv6 address and listening port number for RADIUS authentication server; the “no radius-server authentication host <IPaddress>“ command deletes the RADIUS server

radius-server accounting host <IPaddress> [[port {*<portNum>*}] [primary]] **no radius-server accounting host *<IPaddress>***	Specifies the IP address or IPv6 address and listening port number for RADIUS accounting server; the “no radius-server authentication host <IPaddress>“ command deletes the RADIUS server

3) Configure RADIUS Service parameters.

Command	Explanation
Global Mode	
radius-server dead-time *<minutes>* **no radius-server dead-time**	Configures the restore time when RADIUS server is down; the “no radius-server dead-time” command restores the default setting.
radius-server retransmit *<retries>* **no radius-server retransmit**	Configures the re-transmission times for RADIUS; the “no radius-server retransmit” command restores the default setting
radius-server timeout *<seconds>* **no radius-server timeout**	Configures the timeout timer for RADIUS server; the “no radius-server timeout” command restores the default setting.
radius-server realtime-accounting timer *<minute>*	Set the realtime cost-counting update interval.

14.3 Example of 802.1x Application

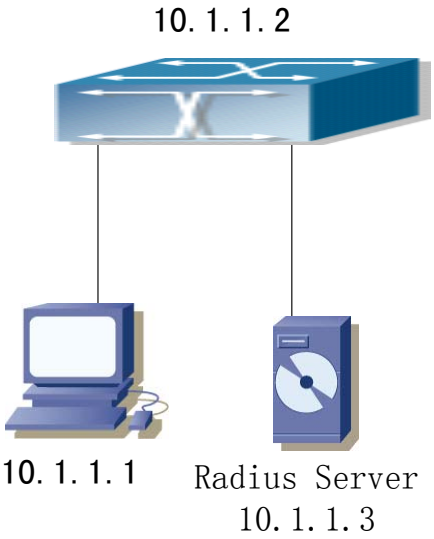


Fig 14-2 IEEE802.1x Configure Topology of the example

The computer is connected to the port 0/0/2 of the switch, and the IEEE802.1 authentication function is enabled on the port, which adopts MAC-address-based authentication as the access method by default. The IP address of the switch is 10.1.1.2, and all the ports other than port 0/0/2 are connected to RADIUS authentication server, the IP address of which is 10.1.1.3. By default the authentication and cost-counting ports are port 1812 and port 1813. The IEEE802.1x authentication client software is installed on the computer to implement IEEE802.1x authentication。

The following is the procedure of configuration
Switch(Config)#interface vlan 1↵
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0↵
Switch(Config-if-vlan1)#exit↵
Switch(Config)#radius-server authentication host 10.1.1.3↵
Switch(Config)#radius-server accounting host 10.1.1.3↵
Switch(Config)#radius-server key test↵
Switch(Config)#aaa enable↵
Switch(Config)#aaa-accounting enable↵
Switch(Config)#dot1x enable↵
Switch(Config)#interface ethernet 0/0/2↵
Switch(Config-Ethernet0/0/2)#dot1x enable↵
Switch(Config-Ethernet0/0/2)#dot1x port-method macbased↵
Switch(Config-Ethernet0/0/2)#dot1x port-control auto↵
Switch(Config-Ethernet0/0/2)#exit

14.4 802.1x Troubleshooting

14.4.1 802.1x Monitor and debug command

14.4.1.1 show aaa config

Command **show aaa config**
Function Displays the configured commands for the switch as a RADIUS client.
Command mode Admin Mode

Displayed information	Description
Is Aaa Enabled	Indicates whether AAA authentication is enabled or not. 1 for enable and 0 for disable.
Is Account Enabled	Indicates whether AAA accounting is enabled or not. 1 for enable and 0 for disable.
MD5 Server Key	Displays the key for RADIUS server.
authentication server sum	The number of authentication servers.

authentication server[X].Host IP .Udp Port .Is Primary .Is Server Dead .Socket No	Displays the authentication server number and corresponding IP address, UDP port number, Primary server or not, down or not, and socket number.
accounting server sum	The number of accounting servers.
accounting server[X].Host IP .Udp Port .Is Primary .Is Server Dead .Socket No	Displays the accounting server number and corresponding IP address, UDP port number, Primary server or not, down or not, and socket number.
Time Out	Displays the timeout value for RADIUS server.
Retransmit	Displays the retransmission times for RADIUS server authentication packets.
Dead Time	Displays the down-restoration time for RADIUS server.
Account Time Interval	Displays accounting time interval.

14.4.1.2 show aaa authenticated-user

Command **show aaa authenticated-user**
Function Displays the authenticated users online.
Command mode Admin Mode

14.4.1.3 show aaa authenticating-user

Command **show aaa authenticating-user**
Function Display the authenticating users.
Command mode Admin Mode

14.4.1.4 show radius count

Command show radius {authencated-user|authencating-user} count
Function Displays the statistics for users of RADIUS authentication.
Parameters authencated-user displays the authenticated users online; **authencating-user** displays the authenticating users.
Command mode Admin Mode

14.4.1.5 show dot1x

Command show dot1x [interface <*interface-list*>]
Function Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.
Parameters **<*interface-list*>** is the port list. If no parameter is specified, information for all ports is

displayed.

Command mode Admin Mode

Displayed information	Explanation
Global 802.1x Parameters	Global 802.1x parameter information
free-resource	Free resource
reauth-enabled	Whether re-authentication is enabled or not
reauth-period	Re-authentication interval
quiet-period	Silent interval
tx-period	EAP retransmission interval
max-req	EAP packet retransmission interval
authenticator mode	Switch authentication mode
Mac Filter	Enables dot1x address filter or not
MacAccessList	Dot1x address filter table
dot1x-EAPoR	Authentication method used by the switch (EAP relay, EAP local end)
dot1x-privateclient	Whether enable private client
dot1x-unicast	Whether enable unicast
802.1x is enabled on ethernet 0/0/8	Indicates whether dot1x is enabled for the port
Authentication Method	Port authentication method (MAC-based, port-based)
Status	Port authentication status
Port-control	Port authorization status
Supplicant	Authenticator MAC address
Max User Number	Max user number of the port
Notify DCBI	Whether has successfully notificated DCBI server or not.

14.4.1.6 debug aaa error

Command debug aaa error

no debug aaa error

Function Enable the debug error information of aaa; the “n **no debug aaa error**” command is used to disable the debug error information of aaa.

Command Mode Admin Mode

Parameters None

14.4.1.7 debug aaa packet

Command debug aaa packet {send|receive|all} interface {[ethernet] <*InterfaceName*>}

no debug aaa packet {send|receive|all} interface {[ethernet] <*InterfaceName*>}

Function Enable the information on receiving/sending packets of aaa; the “no debug aaa packet {send|receive|all} interface {[ethernet] <InterfaceName>}” command is used to disable the information on receiving/sending packets of aaa.

Command Mode Admin Mode

Parameters send represents sending packets; **receive**represents receiving packets; **all** represents receiving and sending packets; ***<InterfaceName>*** is the name of interface.

14.4.1.8 debug aaa detail

Command debug dot1x detail {pkt-send|pkt-receive|internal|userbased|all} interface {[ethernet] *<InterfaceName>*}

no debug dot1x detail {pkt-send|pkt-receive|internal|userbased|all} interface {[ethernet] *<InterfaceName>*}

Function Enable the detail debug information of dot1x; the ” no debug dot1x detail {connection | event | attribute interface {[ethernet] <InterfaceName>}}” command is tgo disable the detail debug information of dot1x.

Command Mode Admin Mode

Parameters pkt-send represents the detail of sending packets; **pkt-receive** represen the details of receiving packets; **internal** represents internal details; **userbased** represents the user-based information; **all** represents all the detailed informations; ***<InterfaceName>*** is the name of interface.

14.4.1.9 debug dot1x error

Command debug dot1x error

no debug dot1x error

Function Enable the information on debug error of dot1x;the “**no debug dot1x error** ” disable the information on debug error of dot1x.

Parameters None

14.4.1.10 debug dot1x packet

Command debug dot1x packet {send|receive|all} interface {[ethernet] *<InterfaceName>*}

no debug dot1x packet {send|receive|all} interface {[ethernet] *<InterfaceName>*}

Function Enable the information on receiving/sending packets of dot1x; the “ no debug dot1x packet {send|receive|all} interface {[ethernet] <InterfaceName>} ” command is to disable the information on receiving/sending packets of dot1x.

Command Mode Admin Mode

Parameters Send represents sending packets; **receive**represents receiving packets; **all** represents receiving and sending packets; ***<InterfaceName>*** is the name of interface.

14.4.1.11 debug dot1x detail

Command debug dot1x detail {pkt-send|pkt-receive|internal|userbased|all} interface {[ethernet] *<InterfaceName>*}

no debug dot1x detail {pkt-send|pkt-receive|internal|userbased|all} interface {[ethernet] *<InterfaceName>*}

Function Enable the detail debug information of dot1x; the ” no debug dot1x detail {connection | event | attribute interface {[ethernet] <InterfaceName>}}” command is tgo disable the detail debug information of dot1x.

Command Mode Admin Mode

Parameters pkt-send represents the detail of sending packets; **pkt-receive** represen the details of receiving packets; **internal** represents internal details; **userbased** represents the user-based information; **all** represents all the detailed informations; ***<InterfaceName>*** is the name of interface.

14.4.1.12 debug dot1x fsm

Command debug dot1x fsm {asm|aksm|ratsm|basm|all} interface {[ethernet] *<InterfaceName>*}

no debug dot1x fsm {asm|aksm|ratsm|basm|all} interface {[ethernet] *<InterfaceName>*}

Function Enable the limited state machine debug information of dot1x; the “no debug dot1x fsm {asm|aksm|ratsm|basm|all} interface {[ethernet] <InterfaceName>} ” command is to disable the limited state machine debug information of dot1x

Command Mode Admin Mode

Parameters asm represents the authenticator state machine information; **aksm** represents the authenticator key transmission state machine state; **ratsm** represents reauthentication timer state machine information; **basm** represents background authentication state machine information; **all** represents all the state machine information; ***<InterfaceName>*** is the name of interface.

14.4.2 802.1x Troubleshooting

It is possible that 802.1x be congfigured on ports and 802.1x authentication be setted to auto, but switch cann’t be to authenticated state after the user runs 802.1x supplicant software. Here are some possible causes and solutions

- If 802.1x cannot be enabled for a port, make sure the port is not executing Spanning tree, or MAC binding, or configured as a Trunk port or for port aggregation. To enable the 802.1x authentication, the above functions must be disabled.
- If the switch is configured properly but still cannot pass through authentication, connectivity between the switch and RADIUS server, the switch and 802.1x client should be verified, and the port and VLAN configuration for the switch should be checked, too.
- Check the event log in the RADIUS server for possible causes. In the event log, not only unsuccessful logins are recorded, but prompts for the causes of unsuccessful login. If the event log indicates wrong authenticator password, radius-server key parameter shall be modified; if the event log indicates no such authenticator, the authenticator needs to be added to the RADIUS server; if the event log indicates no such login user, the user login ID and password may be wrong and should be verified and input again.
- If the access mode of a port is userbased advanced and static user is configured on RADIUS server but is not issued to the switch, first check whether the RADIUS server is configured correctly using the command”ip user helper addres”, and then check whether the RADIUS server configured static user on the port, last check the issueing of static user using the command” show dot1x interface”

Chapter 15 ACL Configuration

15.1 Introduction to ACL

ACL (Access Control List) is an IP packet filtering mechanism employed in switches, providing network traffic control by granting or denying access through the switches, effectively safeguarding the security of networks. The user can lay down a set of rules according to some information specific to packets, each rule describes the action for a packet with certain information matched "permit" or "deny". The user can apply such rules to the incoming or outgoing direction of switch ports, so that data streams in the specific direction of specified ports must comply with the ACL rules assigned.

15.2 Access-list

Access-list is a sequential collection of conditions that corresponds to a specific rule. Each rule consist of filter information and the action when the rule is matched. Information included in a rule is the effective combination of conditions such as source IP, destination IP, IP protocol number and TCP port. Access-lists can be categorized by the following criteria

- Filter information based criterion IP access-list (layer 3 or higher information), MAC access-list (layer 2 information), and MAC-IP access-list (layer 2 or layer 3 or higher).
- Configuration complexity based criterion standard and extended, the extended mode allows more specific filtering of information.
- Nomenclature based criterion numbered and named

  Description of an ACL should cover the above three aspects.

15.2.1 Access-group

When a set of access-lists are created, they can be applied to traffic of any direction on all ports. Access-group is the description to the binding of an access-list to the specified direction on a specific port. When an access-group is created, all packets from in the specified direction through the port will be compared to the access-list rule to decide whether to permit or deny access.

15.2.2 Access-list Action and Global Default Action

There are two access-list actions and default actions "permit" or "deny"

The following rules apply

- An access-list can consist of several rules. Filtering of packets compares packet conditions to the

rules, from the first rule to the first matched rule; the rest of the rules will not be processed.

- Global default action applies only to IP packets in the incoming direction on the ports. For non-incoming IP packets and all outgoing packets, the default forward action is “permit”.
- Global default action applies only when packet flirter is enabled on a port and no ACL is bound to that port, or no binding ACL matches.
- When an access-list is bound to the outgoing direction of a port, the action in the rule can only be “deny”.

15.3 ACL Configuration

15.3.1 ACL Configuration Task Sequence

1. Configuring access-list
   （1） Configuring a numbered standard IP access-list
   （2） Configuring a numbered extended IP access-list
   （3） Configuring a standard IP access-list based on nomenclature
      a) Create a standard IP access-list based on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit ACL Configuration Mode
   （4） Configuring an extended IP access-list based on nomenclature.
      a) Create an extensive IP access-list based on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit ACL Configuration Mode
   （5） Configuring a numbered standard MAC access-list
   （6） Configuring a numbered extended MAC access-list
   （7） Configuring a standard MAC access-list based on nomenclature
      a) Create a standard IP access-list based on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit ACL Configuration Mode
   （8） Configuring a numbered extended MAC-IP access-list
   （9） Configuring a standard MAC-IP access-list based on nomenclature
      a) Create a standard MAC-IP access-list based on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit MAC-IP Configuration Mode
2. Configuring the packet filtering function
   (1) Enable global packet filtering function
   (2) Configure default action.
3. Configuring time range function

(1) Create the name of the time range

(2) Configure periodic time range

(3) Configure absolute time range

4. Bind access-list to a specific direction of the specified port.

1.Configuring access-list

(1) Configuring a numbered standard IP access-list

Command	Explanation
Global Mode	
access-list <*num*> {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} **no access-list <*num*>**	Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list; the "no access-list ***<num>***" command deletes a numbered standard IP access-list.

(2) Configuring a numbered extensive IP access-list

Command	Explanation
Global Mode	
access-list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered ICMP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered IGMP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered TCP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered UDP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.

access-list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered IP extended IP access rule for other specific IP protocol or all IP protocols; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
no access-list <*num*>	Deletes a numbered extensive IP access-list

(3) Configuring a standard IP access-list basing on nomenclature

a. Create a name-based standard IP access-list

Command	Explanation
Global Mode	
ip access-list standard <*name*> **no ip access-list standard <*name*>**	Creates a standard IP access-list based on nomenclature; the "**no ip access-list standard <*name*>** " command delete the name-based standard IP access-list

b. Specify multiple "permit" or "deny" rules

Command	Explanation
Standard IP ACL Mode	
[no] {deny | permit} {{<*sIpAddr*> <*sMask* >} | any-source | {host-source <*sIpAddr*>}}	Creates a standard name-based IP access rule; the "no" form command deletes the name-based standard IP access rule

c. Exit name-based standard IP ACL configuration mode

Command	Explanation
Standard IP ACL Mode	
Exit	Exits name-based standard IP ACL configuration mode

(4) Configuring an name-based extended IP access-list

a. Create an extended IP access-list basing on nomenclature

Command	Explanation
Global Mode	
ip access-list extended <*name*> **no ip access-list extended <*name*>**	Creates an extended IP access-list basing on nomenclature; the "**no ip access-list extended <*name*>** " command deletes the name-based extended IP access-list

b. Specify multiple "permit" or "deny" rules

Command	Explanation
Extended IP ACL Mode	

[no] {deny | permit} icmp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based ICMP IP access rule; the "no" form command deletes this name-based extended IP access rule
[no] {deny | permit} igmp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based IGMP IP access rule; the "no" form command deletes this name-based extended IP access rule
[no] {deny | permit} tcp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} [s-port <*sPort*>] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [d-port <*dPort*>] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based TCP IP access rule; the "no" form command deletes this name-based extended IP access rule
[no] {deny | permit} udp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} [sPort <*s-port*>] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based UDP IP access rule; the "no" form command deletes this name-based extended IP access rule
[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based IP access rule for other IP protocols; the "no" form command deletes this name-based extended IP access rule

c. Exit extended IP ACL configuration mode

Command	Explanation
Extended IP ACL Mode	
Exit	Exits extended name-based IP ACL configuration mode

（5） Configuring a numbered standard MAC access-list

Command	**Explanation**
Global Mode	

access-list <*num*> {deny|permit} {any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} **no access-list <*num*>**	Creates a numbered standard MAC access-list, if the access-list already exists, then a rule will add to the current access-list; the "no access-list ***<num>***" command deletes a numbered standard MAC access-list.

（**6**） Creates a numbered **MAC extended** access-list

Command	**Explanation**
Global Mode	
access-list <*num*> {deny|permit} {any-source-mac | {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[{untagged-eth2|tagged-eth2|untagged-802.3|tagged-802.3} [<*offset1*> <*length1*> <*value1*> [<*offset2*> <*length2*> <*value2*> [<*offset3*> <*length3*> <*value3*> [<*offset4*> <*length4*> <*value4*>]]]]] **no access-list <*num*>**	Creates a numbered MAC extended access-list, if the access-list already exists, then a rule will add to the current access-list; the "no access-list ***<num>***" command deletes a numbered MAC extended access-list.

（**7**） Configuring a extended **MAC** access-list based on nomenclature

a. Create a extended **MAC** access-list based on nomenclature

Command	**Explanation**
Global Mode	
mac-access-list extended <*name*> **no mac-access-list extended <*name*>**	Creates an extended name-based MAC access list; the "no" form command deletes this name-based extended MAC access list

b. Specify multiple "permit" or "deny" rule entries

Command	**Explanation**
Extended name-based MAC access rule Mode	
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>} |{<*dmac*> <*dmac-mask*>}} [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]] [ethertype <*protocol*> [<*protocol-mask*>]]	Creates an extended name-based MAC access rule matching MAC frame; the "no" form command deletes this name-based extended MAC access rule

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [untagged-eth2 [ethertype <*protocol*> [protocol-mask]]]	Creates an extended name-based MAC access rule matching untagged ethernet 2 frame; the "**no**" form command deletes this name-based extended MAC access rule
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [untagged-802.3]	Creates an MAC access rule matching 802.3 frame; the "no" form command deletes this MAC access rule
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[tagged-eth2 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]] [ethertype<*protocol*> [<*protocol-mask*>]]]	Creates an MAC access rule matching tagged ethernet 2 frame; the "no" form command deletes this MAC access rule
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [tagged-802.3 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]]]	Creates an MAC access rule matching tagged 802.3 frame;the "no" form command deletes this MAC access rule

c. Exit ACL Configuration Mode

Command	**Explanation**
Extended name-based MAC access configure Mode	
Exit	Quit the extended name-based MAC access configure mode

(8) Configuring a numbered extended MAC-**IP** access-list

Command	**Explanation**
Global mode	

access-list<*num*>{deny|permit}{any-source-mac | {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp {{<*source*><*source-wildcard*>}|any-source | {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination | {host-destination<*destination-host-ip*>}}[<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered mac-icmp extended mac-ip access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<*num*>{deny|permit}{any-source-mac | {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp {{<*source*><*source-wildcard*>}|any-source | {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination | {host-destination<*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered mac-igmp extended mac-ip access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<num>{deny|permit}{any-source-mac | {host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source | {host-source<source-host-ip>}}[s-port<port1>] {{<destination><destination-wildcard>}|any-destination | {host-destination <destination-host-ip>}} [d-port <port3>] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>][time-range<*time-range-name*>]	Creates a numbered extended mac-tcp access rule for other specific mac-tcp protocol or all mac-tcp protocols; if the numbered extended access-list of specified number
access-list<*num*>{deny|permit}{any-source-mac | {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}udp {{<*source*><*source-wildcard*>}|any-source | {host-source<*source-host-ip*>}}[s-port<*port1*>] {{<*destination*><*destination-wildcard*>}|any-destination | {host-destination<*destination-host-ip*>}} [d-port <*port3*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered extended mac-ip access rule for other specific mac-ip protocol or all mac-ip protocols; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.

access-list<*num*>{deny|permit}{any-source-mac | {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source | {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination | {host-destination<*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered extended mac-ip access rule for other specific mac-ip protocol or all mac-ip protocols; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
no access-list <*num*>	Deletes this nunbered extended MAC-IP access rule

9)Configuring a extended MAC-**IP** access-list based on nomenclature

a) Create a extended **MAC-IP** access-list based on nomenclature

Command	**Explanation**
Global Mode	
mac-ip-access-list extended <*name*> **no mac-ip-access-list extended <*name*>**	Creates an extended name-based MAC-IP access rule; the “no” form command deletes this name-based extended MAC-IP access rule

b) Specify multiple “permit” or “deny” rule entries

Command	**Explanation**
Extended name-based MAC-IP access Mode	
[no] {deny|permit} {any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp {{<*source*><*source-wildcard*>}|any-source | {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination | {host-destination <*destination-host-ip*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based MAC-ICMP access rule; the “no” form command deletes this name-based extended MAC-ICMP access rule

[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp {{<*source*><*source-wildcard*>}|any-source | {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination | {host-destination <*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based MAC-IGMP access rule; the "no" form command deletes this name-based extended MAC-IGMP access rule
[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source | {host-source<source-host-ip>}}[s-port<port1>] {{<destination><destination-wildcard>}|any-destination | {host-destination <destination-host-ip>}} [d-port <port3>] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>][time-range<*time-range-name*>]	Creates an extended name-based MAC-TCP access rule; the "no" form command deletes this name-based extended MAC-TCP access rule
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}udp {{<*source*><*source-wildcard*>}|any-source | {host-source<*source-host-ip*>}}[s-port<*port1*>] {{<*destination*><*destination-wildcard*>}|any-destination | {host-destination <*destination-host-ip*>}} [d-port <*port3*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based MAC-UDP access rule; the "no" form command deletes this name-based extended MAC-UDP access rule
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source | {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination | {host-destination<*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based mac-ip access rule for the other IP protocol; the "no" form command deletes this name-based mac-ip extended access rule

c) Exit **MAC-IP** Configuration Mode

Command	**Explanation**
Extended name-based MAC-IP access Mode	

Exit	Quit extended name-based MAC-IP access mode

2. Configuring packet filtering function

(1)Enable global packet filtering function

Command	Explanation
Global Mode	
Firewall enable	Enables global packet filtering function
Firewall disable	disables global packet filtering function

(2)Configure default action

Command	Explanation
Global Mode	
Firewall default permit	Sets default action to “permit”
Firewall default deny	Sets default action to “deny”

3. Configuring time range function

(1)Create the name of the time range

Command	Explanation
Global Mode	
time-range <*time_range_name*>	Create a time range named *time_range_name*
no time-range <*time_range_name*>	Stop the time range function named ***time_range_name***

(2) Configure **periodic time range**

Command	Explanation
Time range Mode	
absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<*start_time*>to {Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday} <*end_time*>	Configure the time range for the request of the week,and every week will run by the time range
periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday} | daily | weekdays | weekend} <*start_time*> to <*end_time*>	

[no]absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<*start_time*> to{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday | Sunday} <*end_time*>	stop the function of the time range in the week
[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|daily|weekdays | weekend} <*start_time*> to <*end_time*>	

(3)Configure absolute time range

Command	Explanation
Global Mode	
Absolute start<*start_time*><*start_data*>[end<*end_time*> <*end_data*>]	Configure absolute time range
[no]absolute start<*start_time*><*start_data*>[end<*end_time*><*end_data*>]	stop the function of the time range

4. Bind access-list to a specific direction of the specified port

Command	Explanation
Physical Interface Mode, VLAN interface Mode	
{ip|mac|mac-ip} access-group <*acl-name*> {in|out} **no {ip|mac|mac-ip} access-group <*acl-name*> {in|out}**	Applies an access-list to the specified direction on the port; the "**no {ip|mac|mac-ip} access-group <*acl-name*> {in|out}**" command deletes the access-list bound to the port.

15.4 ACL Example

Scenario 1

The user has the following configuration requirement port 1/10 of the switch connects to 10.0.0.0/24 segment, ftp is not desired for the user.

Configuration description

a) Create a proper ACL
b) Configuring packet filtering function
c) Bind the ACL to the port

The configuration steps are listed below Switch(Config)#access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
Switch(Config)#firewall enable
Switch(Config)#firewall default permit

Switch(Config)#interface ethernet 0/0/10
Switch(Config-Ethernet0/0/10)#ip access-group 110 in
Switch(Config-Ethernet0/0/10)#exit
Switch(Config)#exit

Configuration result

Switch#show firewall
Firewall is enabled.
Firewall default rule is to permit any packet.
Switch#show access-lists
access-list 110(used 1 time(s))
access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch#show access-group interface ethernet 0/0/10
interface name Ethernet0/0/10
the ingress acl use in firewall is 110.

Scenario 2

The user has the following configuration requirement port 1/10 of the switch connects to 00-12-11-23-XX-XX segment, 802.3 is not desired for the user.

Configuration description

a)Create a proper ACL
b)Configuring packet filtering function
c)Bind the ACL to the port

The configuration steps are listed below
Switch(Config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac untagged-802.3
Switch(Config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac tagged-802.3
Switch(Config)#firewall enable
Switch(Config)#firewall default permit

Switch(Config)#interface ethernet 0/0/10
Switch(Config-Ethernet0/0/10)#ip access-group 1100 in

Switch(Config-Ethernet0/0/10)#exit
Switch(Config)#exit

Configuration result

Switch#show firewall
Firewall is enabled.
Firewall default rule is to permit any packet.
Switch #show access-lists
access-list 1100(used 1 time(s))
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-FF-FF any-destination-mac untagged-802.3
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-FF-FF any-destination-mac tagged-802.3
Switch #show access-group
interface name Ethernet0/0/10
MAC Ingress access-list used is 1100.

Scenario 3

The user has the following configuration requirement port 1/10 of the switch connects to 00-12-11-23-XX-XX segment, IP is 10.0.0.0/24 segment , ftp is not desired for the user.

Configuration description

a)Create a proper ACL
b)Configuring packet filtering function
c)Bind the ACL to the port

The configuration steps are listed below

Switch(Config)#access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-FF-FF any-destination-mac tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch(Config)#firewall enable
Switch(Config)#firewall default permit

Switch(Config)#interface ethernet 0/0/10
Switch(Config-Ethernet0/0/10)#mac-ip access-group 3110 in
Switch(Config-Ethernet0/0/10)#exit
Switch(Config)#exit

Configuration result

Switch#show firewall
Firewall is enabled.
Firewall default rule is to permit any packet.

Switch#show access-lists
access-list 3110(used 1 time(s))
access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-FF-FF any-destination-mac tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch #show access-group
interface name Ethernet0/0/10
MAC-IP Ingress access-list used is 3110.

15.5 ACL Troubleshooting

15.5.1 Monitor And Debug Command

15.5.1.1 show access-lists

Command **show access-lists [<*num*>|<*acl-name*>]**
Functions Reveal ACL of configuration
Parameters **<*acl-name*>**, specific ACL name character string; **<*num*>,** specific ACL No.
Default None
Command Mode Admin mode

Displayed information	Explanation
access-list 10(used 0 time(s))	Number ACL10, 0 time to be used
access-list 10 deny any-source	Deny any IP packets to pass
access-list 100(used 1 time(s))	Nnumber ACL10, 1 time to be used
access-list 100 deny ip any-source any-destination	Deny IP packet of any source IP address and destination address to pass
access-list 100 deny tcp any-source any-destination	Deny TCP packet of any source IP address and destination address to pass
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800	Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets whose 15th and 16th byte is respectively 0x08 , 0x0 to pass
access-list 3100 permit any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000	Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100 and destination interface 40000

15.5.1.2 show access-group

Command **show access-group [interface [Ethernet] <*name*>]**
Functions Reveal tying situation of ACL on port

Parameters ***<name>,***Interface name
Default None
Command Mode Admin mode

Displayed information	Explanation
interface name Ethernet0/0/2	Tying situation on port Ethernet0/0/2
IP Ingress access-list used is 111	No. 111 numeric expansion ACL tied to entrance of port Ethernet0/0/2
interface name Ethernet0/0/1	Tying situation on port Ethernet0/0/1
IP Ingress access-list used is 10	No. 10 standard expansion ACL tied to entrance of port Ethernet0/0/1

15.5.1.3 show firewall

Command **show firewall**
Functions Reveal configuration information of packet filtering functions
Parameters None
Default None
Command Mode Admin mode

Displayed information	Explanation
fire wall is enable	Packet filtering function enabled
the default action of firewall is permit	Default packet filtering function is permit

15.5.1.4 show time-range

Command **show time-range<*word*>**
Functions Reveal configuration information of time range functions
Parameters ***word*** assign name of time-range needed to be revealed
Default None

15.5.2 ACL Troubleshooting

- The check of list entris in ACL is a top-down behavior, once one entry is mached, the check will be finished immediately;
- Only when there is no ACL binded or no ACL entry mached on the special direction of the port, the default rules will be used;
- Each port ingress can bind one MAC-IP ACL or one IP ACL or one MAC ACL;
- Each port egress can bind one MAC-IP ACL or one IP ACL or one MAC ACL
- When two sets of ACL are binded to the ingress and egress simultaneously, the priority of the egress rules is higher than that of ingress rules; in the same set of ACL, the earlier the rule is configurated, the higher its priority is;
- When one ACL is binded to egress direction of the port, it can only include deny list entries;
- Only the interfaces on the MASTER switch can support the binding of ACL;

- The number of ACL that can be binded successfully is dependent on the content of binded ACL and the limitation of hardware resource;
- If there are some rules including the same filtering information but conflicting behavior in the access-list, it can not be binded to the port, and will cause an error prompt. For example configure permit tcp any-source any-destination and deny tcp any-source any-destination at the same time.

Chapter 16 AM Configuration

16.1 AM Introduction

AM(access management) compares the information of the received data message (source IP address or source IP + source MAC) with the configured hardware address pool, if founds a match, forwards the message, if not, dumps it.

16.2 AM pool

AM pool is an address list, each entry of this address list corresponds with a user. Each entry contains address information and its corresponding port. There two kinds of address information

IP address(ip-pool), specifies the user's source IP address information of the port.

MAC-IP address (mac-ip pool)，specifies the user's source MAC address and source IP address information of the port.

The default AM action is to deny. When the AM is enabled, the AM module will deny all the IP messages(only allows the source addresses of the members of the IP pool), when AM is disabled, it will delete all the address pools.

16.3 AM Configuration

16.3.1 AM Configuration Task Sequence

1. Enable AM
2. Configure IP address on an interface
3. Configure MAC-IP address on an interface
4. Delete all the address pools

1. Enable AM

Command	**Explanation**
Global configuration mode	
am enable **no am enable**	Enable the AM access management function to configure address pools. The "no am enable" command will disable AM and delete all the address pools.

2. Configure IP address on an interface

Command	Explanation
Physical interface configuration mode	
am port **no am port**	Enable or disable the AM function of a physical interface.
am ip-pool <*start_ip_address*> [<*num*>] **no am ip-pool <*start_ip_address*> [<*num*>]**	Configure IP address on a physical interface. The “no am ip-pool <start_ip_address> [<num>] ” command will delete all the configured IP addresses on the interface.

3. Configure MAC-IP address on an interface

Command	Explanation
Physical interface configuration mode	
am mac-ip-pool<mac_*address*> <*ip_address*> **no am mac-ip-pool <mac_*address*>< *ip_address*>**	Configure MAC-IP address on a physical interface. The “no am mac-ip-pool <mac_address>< ip_address>” command will delete all the configured MAC-IP addresses on the interface.

4.Delete all the address pools

Command	Explanation
Global configuration mode	
no am all {ip-pool|mac-ip-pool}	Delete all the MAC-IP pools or IP pools configured by the users.

16.4 AM Examples

Scenario 1

The configuration demand of the user is that the port 10 of the switch connects to the 10.1.1.0/8 segment, the administrator hopes that 8 IP addresses from 10.1.1.1 to 10.1.1.8 8 can be allowed to access Internet.

Change Configuration

1. Enable AM function;
2. Configure IP pool;

The following is the configuration procedure

Switch(Config)#am enable

```
Switch(Config)#interface ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#am port
Switch(Config-Ethernet0/0/1)#am ip-pool 10.1.1.1 8
Switch(Config-Ethernet0/0/1)#exit
Switch(Config)#exit
```

Configuration result

```
Switch#show am
Global AM is enabled
Interface Ethernet0/0/1 am is enable
Interface Ethernet0/0/1
    am ip-pool 10.1.1.1    8 USER_CONFIG
```

Scenario 2

The configuration demand of the user is that the port 10 of the switch connects to the 10.1.1.0/8 segment, the administrator hopes the binding relationships between users and MAC+IP are user1(100.1.1.1，00-00-00-00-01-12),user2(100.1.1.2，00-00-00-00-00-13).

Change Configuration

1. Enable AM function;
2. Configure MAC-IP pool;

The following is the configuration procedure

```
Switch(Config)#am enable
Switch(Config)#interface ethernet 0/0/10
Switch(Config-Ethernet0/0/10)#am port
Switch(Config-Ethernet0/0/10)#am mac-ip-pool 00-00-00-00-01-12 100.1.1.1
Switch(Config-Ethernet0/0/10)#am mac-ip-pool 00-00-00-00-00-13 100.1.1.2
Switch(Config-Ethernet0/0/10)#exit
Switch(Config)#exit
```

Configuration result

```
Switch#show am
    Global AM is enabled
Interface Ethernet0/0/10 am is enable
Interface Ethernet0/0/10
        am mac-ip-pool    00-00-00-00-00-13 100.1.1.2 USER_CONFIG
        am mac-ip-pool    00-00-00-00-01-12 100.1.1.1 USER_CONFIG
```

16.5 AM Troubleshooting

16.5.1 AM Debug and Monitor Command

16.5.1.1 show am

Command show am [interface <interfaceName>]
Function Display the address entries configured on the current switch.
Parameters interfaceName name of the physical interface
Command Mode Global configuration mode
Default Setting None

Displayed information	Explanation
Global AM is enabled	AM is enabled
am mac-ip-pool 00-00-00-00-00-13 100.1.1.2 USER_CONFIG	Only the users whose source MAC = 00-00-00-00-00-13 and source IP=100.1.1.2 can pass, this is configured by users.
am mac-ip-pool 00-00-00-00-01-12 100.1.1.1 USER_CONFIG	Only the users whose source MAC = 00-00-00-00-01-12 and source IP=100.1.1.1can pass, this is configured by users.
am ip-pool 10.1.1.1 8 USER_CONFIG	Only the users whose source IP=10.1.1.1～10.1.1.8 can pass, this is configured by users.

16.5.2 AM Troubleshooting

- Since there is only limited hardware resources for AM, each port can configure 507 entries at most.
- The AM resource requires that the IP addresses and MAC addresses configured by users cannot conflict, that is the different users on the same switch cannot have the same IP or MAC configuration.

Chapter 17 Port Channel Configuration

17.1 Introduction to Port Channel

To understand Port Channel, Port Group should be introduced first. Port Group is a group of physical ports in the configuration level; only physical ports in the Port Group can take part in link aggregation and become a member port of a Port Channel. Logically, Port Group is not a port but a port sequence. Under certain conditions, physical ports in a Port Group perform port aggregation to form a Port Channel that has all the properties of a logical port, therefore it becomes an independent logical port. Port aggregation is a process of logical abstraction to abstract a set of ports (port sequence) with the same properties to a logical port. Port Channel is a collection of physical ports and used logically as one physical port. Port Channel can be used as a normal port by the user, and can not only add network's bandwidth, but also provide link backup. Port aggregation is usually used when the switch is connected to routers, PCs or other switches.

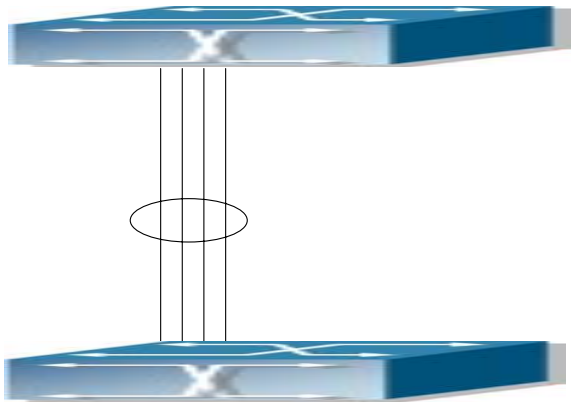


Fig 17-1 Port aggregation

As shown in the above figure, Switch1 is aggregated to a Port Channel, the bandwidth of this Port Channel is the total of all the four ports. If traffic from SwitchA needs to be transferred to SwitchB through the Port Channel, traffic allocation calculation will be performed based on the source MAC address and the lowest bit of target MAC address. The calculation result will decide which port to convey the traffic. If a port in Port Channel fails, the other ports will undertake traffic of that port through a traffic allocation algorithm. This algorithm is carried out by the hardware.

SS2R24/48G4i switch switch offers 2 methods for configuring port aggregation manual Port Channel creation and LACP (Link Aggregation Control Protocol) dynamic Port Channel creation. Port aggregation can only be performed on ports in full-duplex mode.

For Port Chansnel to work properly, member ports of the Port Channel must have the same properties as follows

- All ports are in full-duplex mode.
- All Ports are of the same speed.

- All Ports are of the same type
- All ports are Access ports and belong to the same VLAN or are all Trunk ports.
- If the ports are Trunk ports, then their “Allowed VLAN” and “Native VLAN” property should also be the same.

If Port Channel is configured manually or dynamically on SS2R24/48G4i switch switch, the system will automatically set the port with the smallest number to be Master Port of the Port Channel. If the spanning tree function is enabled in the switch, the spanning tree protocol will regard Port Channel as a logical port and send BPDU frames via the master port.

Port aggregation is closely related with switch hardware. SS2R24/48G4i switch switch allow physical port aggregation of any two switches, maximum 8 port groups and 8 ports in each port group are supported.

Once ports are aggregated, they can be used as a normal port. SS2R24/48G4i switch switch have a built-in aggregation interface configuration mode, the user can perform related configuration in this mode just like in the VLAN and physical port configuration mode.

17.2 Port Channel Configuration

17.2.1 Port Channel Debug and Monitor Command

1. Create a port group in Global Mode.
2. Add ports to the specified group from the Port Mode of respective ports.
3. Enter port-channel configuration mode.

1. Creating a port group

Command	Explanation
Global Mode	
port-group *<port-group-number>* [load-balance { dst-src-mac }] **no port-group <port-group-number> [load-balance]**	Creates or deletes a port group and sets the load balance method for that group.

2. Add physical ports to the port group

Command	Explanation
Interface Mode	
port-group *<port-group-number>* mode {active|passive|on} **no port-group *<port-group-number>***	Adds ports to the port group and sets their mode.

3. Enter port-channel configuration mode.

Command	Explanation
Global Mode	
interface port-channel *<port-channel-number>*	Enters port-channel configuration mode.

17.3 Port Channel Example

Scenario 1 Configuring Port Channel in LACP.

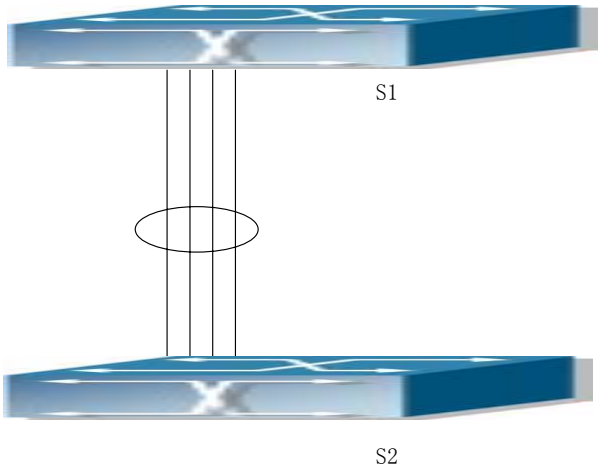


Fig 17-2 Configuring Port Channel in LACP

Example The switches in the description below are all SS2R24/48G4i switch switch and as shown in the figure, ports 1, 2, 3 of Switch1 are access ports that belong to vlan1. Add those three ports to group1 in active mode. Ports 6, 7, 8 of Switch2 are trunk ports that also belong to vlan1,and allow all. Add these three ports to group2 in passive mode. All the ports should be connected with cables

The configuration steps are listed below

Switch1#config
Switch1 (Config)#interface eth 0/0/1-3
Switch1 (Config-Port-Range)#port-group 1 mode active
Switch1 (Config-Port-Range)#exit
Switch1 (Config)#interface port-channel 1
Switch1 (Config-If-Port-Channel1)#

Switch2#config
Switch2 (Config)#port-group 2
Switch2 (Config)#interface eth 0/0/6
Switch2 (Config-Ethernet0/0/6)#port-group 2 mode passive
Switch2 (Config-Ethernet0/0/6)#exit
Switch2 (Config)# interface eth 0/0/8-9
Switch2 (Config-Port-Range)#port-group 2 mode passive
Switch2 (Config-Port-Range)#exit
Switch2 (Config)#interface port-channel 2
Switch2 (Config-If-Port-Channel2)#

Configuration result

Shell prompts ports aggregated successfully after a while, now ports 1, 2, 3of Switch 1 form an aggregated port named “Port-Channel1”, ports 6, 7, 8 of Switch 2 forms an aggregated port named “Port-Channel2”; configurations can be made in their respective aggregated port configuration mode.

Scenario 2 Configuring Port Channel in ON mode.

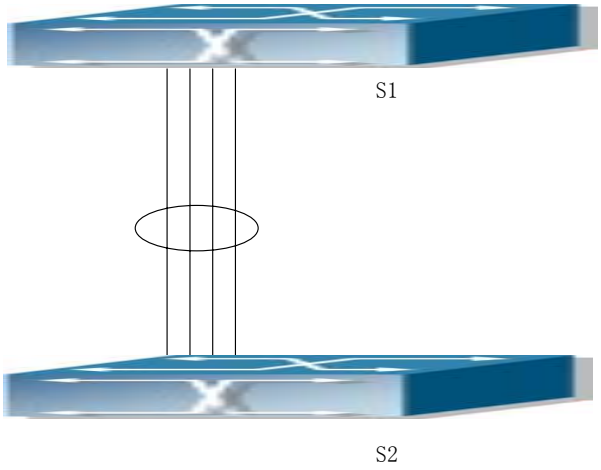


Fig 17-3 Configuring Port Channel in ON mode

Example As shown in the figure, ports 1, 2, 3 of Switch1 are access ports that belong to vlan1. Add those three port to group1 in “on” mode. Ports 6, 7, 8 of Switch2 are trunk ports that also belong to vlan1, and allow all,and add the these four ports to group2 in “on” mode

The configuration steps are listed below

Switch1#config
Switch1 (Config)#interface eth 0/0/1
Switch1 (Config-Ethernet0/0/1)# port-group 1 mode on
Switch1 (Config-Ethernet0/0/1)#exit
Switch1 (Config)#interface eth 0/0/2
Switch1 (Config-Ethernet0/0/2)# port-group 1 mode on
Switch1 (Config-Ethernet0/0/2)#exit
Switch1 (Config)#interface eth 0/0/3
Switch1 (Config-Ethernet0/0/3)# port-group 1 mode on
Switch1 (Config-Ethernet0/0/3)#exit

Switch2#config
Switch2 (Config)#port-group 2
Switch2 (Config)#interface eth 0/0/6
Switch2 (Config-Ethernet0/0/6)#port-group 2 mode on
Switch2 (Config-Ethernet0/0/6)#exit
Switch2 (Config)# interface eth 0/0/8-9
Switch2 (Config-Port-Range)#port-group 2 mode on
Switch2 (Config-Port-Range)#exit

Configuration result

Add ports 1, 2, 3 of Switch 1 to port-group 1 in order, and we can see a group in “on” mode is completely joined forcedly, switch in other ends won’t exchange LACP BPDU to complete aggregation. Aggregation finishes immediately when the command to add port 2 to port-group 1 is entered, port 1 and port 2 aggregate to be port-channel 1, when port 3 joins port-group 1, port-channel 1 of port 1 and 2

are ungrouped and re-aggregate with port 3 to form port-channel 1. (It should be noted that whenever a new port joins in an aggregated port group, the group will be ungrouped first and re-aggregated to form a new group.) Now all four ports in both SwitchA and SwitchB are aggregated in “on” mode and become an aggregated port respectively.

17.4 Port Channel Troubleshooting

17.4.1 Debug and Monitor Command

17.4.1.1 show port-group

Command show port-group [*<port-group-number>*] {brief | detail | load-balance | port | port-channel}

Parameters ***<port-group-number>*** is the group number of port channel to be displayed, from 1 to 8; **“brief”** displays summary information; **“detail”** displays detailed information; **“load-balance”** displays load balance information; **“port”** displays member port information; **“port-channel”** displays port aggregation information.

Command mode Admin Mode

1. Display summary information for port-group 1.

Displayed information	Explanation
Number of ports in group	Port number in the port group
Maxports	Maximum number of ports allowed in a group
Number of port-channels	Whether aggregated to port channel or not
Max port-channels	Maximum port channel number can be formed by port group.

2. Display detailed information for port-group 1

Displayed information	Explanation
portnumber	Port number
actor_port_agg_id	The channel number to add the port to. If the port cannot be added to the channel due to inconsistent parameters between the port and the channel, 3 will be displayed.
partner_oper_sys	System ID of the other end.
partner_oper_key	Operational key of the other end.
actor_oper_port_key	Local end operational key
mode of the port	The mode in which port is added to the group
mac_type	Port type standard Ethernet port and fiber-optical distributed data interface

speed_type	Port speed type 10Mbps, 100Mbps, 1,000Mbps and 10Gbps.
duplex_type	Port duplex mode full-duplex and half-duplex
port_type	Port VLAN property access port or trunk port
mux_state	Status of port binding status machine
rcvm_state	Status of port receiving status machine
prm_state	Status of port sending status machine

3. Display load balance information for port-group 1.

4. Display member port information for port-group 1.

Displayed information	**Explanation**
portnumber	Port number
port priority	Port Priority
system	System ID
system priority	System Priority
LACP activety	Whether port is added to the group in “active” mode, 1 for yes.
LACP timeout	Port timeout mode, 1 for short timeout.
Aggregation	Whether aggregation is possible for the port, 0 for independent port that does not allow aggregation.
Synchronization	Whether port is synchronized with the partner end.
Collecting	Whether status of port bound status machine is “collecting” or not.
Distributing	Whether status of port bound status machine is “distributing” or not.
Defaulted	Whether the local port is using default partner end parameter.
Expired	Whether status of port receiving status machine is “expire” or not.
Selected	Whether the port is selected or not..

5. Display port-channel information for port-group1

Displayed information	**Explanation**
Port channels in the group	If port-channel does not exist, the above information will not be displayed.
Number of port	Port number in the port-channel.
Standby port	Port that is in “standby” status, which means the port is qualified to join the channel but cannot join the channel due to the maximum port limit, thus the port status is “standby” instead of “selected”.

17.4.1.2 debug lacp

Command **debug lacp**
no debug lacp
Function Enables the LACP debug function "**no debug lacp"** command disables this debug function**.**
Command mode Admin Mode
Default LACP debug information is disabled by default.

17.4.2 Port Channel Channel Troubleshooting

If problems occur when configuring port aggregation, please first check the following for causes.

- Ensure all ports in a port group have the same properties, i.e., whether they are in full-duplex mode, forced to the same speed, and have the same VLAN properties, etc. If inconsistency occurs, make corrections.
- Some commands cannot be used on a port in port-channel, such as arp, bandwidth, ip, ip-forward, etc.
- When port-channel is forced, as the aggregation is triggered manually, the port group will stay unaggregated if aggregation fails due to inconsistent VLAN information. Ports must be added to or removed from the group to trigger another aggregation, if VLAN information inconsistency persists, the aggregation will fail again. The aggregation will only succeed when VLAN information is consistent and aggregation is triggered due to port addition or removal.
- Verify that port group is configured in the partner end, and in the same configuration. If the local end is set in manual aggregation or LACP, the same should be done in the partner end; otherwise port aggregation will not work properly. Another thing to be noted is that if both ends are configured with LACP, then at least one of them should be in ACTIVE mode, otherwise LACP packet won't be initiated.
- LACP cannot be used on ports with Security and IEEE 802.1x enabled.
- Once the port-channel created, all the configuration of the ports can only be applied to port-channel ports
- LACP should be mutually exclusive to Security and 802.1X ports, if a port has been configured with the two protocols above, the LACP is not allowed to be enabled.

Chapter 18 DHCP Configuration

18.1 Introduction to DHCP

DHCP [RFC2131] is the acronym for Dynamic Host Configuration Protocol. It is a protocol that assigns IP address dynamically from the address pool as well as other network configuration parameters such as default gateway, DNS server, and default route and host image file position within the network. DHCP is the enhanced version of BootP. It is a mainstream technology that can not only provide boot information for diskless workstations, but can also release the administrators from manual recording of IP allocation and reduce user effort and cost on configuration. Anther benefit of DHCP is it can partially ease the pressure on IP demands, when the user of an IP leaves the network that IP can be assigned to another user.

DHCP is a client-server protocol, the DHCP client requests the network address and configuration parameters from the DHCP server; the server provides the network address and configuration parameters for the clients; if DHCP server and clients are located in different subnets, DHCP relay is required for DHCP packets to be transferred between the DHCP client and DHCP server. The implementation of DHCP is shown below

Fig 18-1 DHCP protocol interaction

Explanation

1. DHCP client broadcasts DHCPDISCOVER packets in the local subnet.
2. On receiving the DHCPDISCOVER packet, DHCP server sends a DHCPOFFER packet along with IP address and other network parameters to the DHCP client.
3. DHCP client broadcast DHCPREQUEST packet with the information for the DHCP server it selected after selecting from the DHCPOFFER packets.
4. The DHCP server selected by the client sends a DHCPACK packet and the client gets an IP address and other network configuration parameters.

The above four steps finish a Dynamic host configuration assignment process. However, if the DHCP server and the DHCP client are not in the same network, the server will not receive the DHCP broadcast packets sent by the client, therefore no DHCP packets will be sent to the client by the server. In this case, a DHCP relay is required to forward such DHCP packets so that the DHCP packets exchange can be completed between the DHCP client and server.

SS2R24/48G4i switch switch can act as both a DHCP server and a DHCP relay. DHCP server

DHCPDisco

DHCPOFF

DHCPREQUE

supports not only dynamic IP address assignment, but also manual IP address binding (i.e. specify a specific IP address to a specified MAC address or specified device ID over a long period. The differences and relations between dynamic IP address allocation and manual IP address binding are 1) IP address obtained dynamically can be different every time; manually bound IP address will be the same all the time. 2) The lease period of IP address obtained dynamically is the same as the lease period of the address pool, and is limited; the lease of manually bound IP address is theoretically endless. 3) The IP addresses bound manually have higher priority than the IP addresses allocated dynamically. 4) Dynamic DHCP address pool can inherit the network configuration parameters of the dynamic DHCP address pool of the related segment.

18.2 DHCP Server Configuration

18.2.1 DHCP Sever Configuration Task List

1. Enable/Disable DHCP server
2. Configure DHCP Address pool
   (1) Create/Delete DHCP Address pool
   (2) Configure DHCP address pool parameters
   (3) Configure manual DHCP address pool parameters
3. Enable logging for address conflicts
4. Configure count of ping packets and out time

1.Enable/Disable DHCP server

Command	**Explanation**
Global Mode	
service dhcp **no service dhcp**	Enables DHCP server

2. Configure DHCP Address pool

(1) Create/Delete DHCP Address pool

Command	**Explanation**
Global Mode	
ip dhcp pool <*name*> **no ip dhcp pool <*name*>**	Configures DHCP Address pool

(2)Configure DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
network-address <*network-number*> [mask | prefix-length] **no network-address**	Configures the address scope that can be allocated to the address pool
default-router [address1[address2[…address8]]] **no default-router**	Configures default gateway for DHCP clients

dns-server [address1[address2[…address8]]] **no dns-server**	Configures DNS server for DHCP clients
domain-name <*domain*> **no domain-name**	Configures Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.
netbios-name-server [address1[address2[…address8]]] **no netbios-name-server**	Configures the address for WINS server
netbios-node-type {**b-node|h-node|m-node|p-node|<*type-number*>**} **no netbios-node-type**	Configures node type for DHCP clients
bootfile <*filename*> **no bootfile**	Configures the file to be imported for DHCP clients on boot up
next-server [address1[address2[…address8]]] **no next-server [address1[address2[…address8]]]**	Configures the address of the server hosting file for importing
option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>} **no option <*code*>**	Configures the network parameter specified by the option code
lease (infinite | <0-365>days (<0-23>hours (<0-59>minutes|)|))no lease	Configures the lease period allocated to addresses in the address pool
Global Mode	
ip dhcp excluded-address <*low-address*> [<*high-address*>] **no ip dhcp excluded-address <*low-address*> [<*high-address*>]**	Excludes the addresses in the address pool that are not for dynamic allocation.

(3) Configure manual DHCP address pool parameters

Command	**Explanation**
DHCP Address Pool Mode	
hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}] **no hardware-address**	Specifies the hardware address when assigning address manually
host <*address*> [<*mask*> | <*prefix-length*>] **no host**	Specifies the IP address to be assigned to the specified client when binding address manually
client-identifier <*unique-identifier*> **no client-identifier**	Specifies the unique ID of the user when binding address manually
client-name <*name*> **no client-name**	Configures a client name when binding address manually

3.Enable logging for address conflicts

Command	**Explanation**

Global Mode	
ip dhcp conflict logging **no ip dhcp conflict logging**	Enables logging for DHCP address to detect address conflicts
Admin Mode	
clear ip dhcp conflict <*address* | *all*>	Deletes a single address conflict record or all conflict records

4. Configure count of ping packets and out time

Command	**Explanation**
Global Mode	
ip dhcp ping packets <*count*> **no ip dhcp ping packets**	Configure count of ping packets to be be assigned in DHCP Address pool
ip dhcp ping timeout <*milliseconds*> **no ip dhcp ping timeout**	Configure timeout time after set ping packets to receive responses

18.2.2 DHCP Server Configuration Commands Example

Scenario 1

Too save configuration efforts of network administrators and users, a company is using SS2R24/48G4i switch switch as a DHCP server. The Admin VLAN IP address is 10.16.1.2/24. The local area network for the company is divided into network A and B according to the office locations. The network configurations for location A and B are shown below.

PoolA(network 10.16.1.0)		**PoolB(network 10.16.2.0)**	
Device	IP address	Device	IP address
Default gateway	10.16.1.200 10.16.1.201	Default gateway	10.16.1.200 10.16.1.201
DNS server	10.16.1.202	DNS server	10.16.1.202
WINS server	10.16.1.209	WINS server	10.16.1.209
WINS node type	H-node	WINS node type	H-node
Lease	3 days	Lease	1 days

In location A, a machine with MAC address 00-03-22-23-dc-ab is assigned with a fixed IP address of 10.16.1.210 and named as “management”.

```
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 10.16.1.2 255.255.255.0
Switch(Config--If-Vlan1)#exit
Switch(Config)#ip dhcp pool A
Switch(dhcp-A-config)#network 10.16.1.0 24
Switch(dhcp-A-config)#lease 3
Switch(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201
Switch(dhcp-A-config)#dns-server 10.16.1.202
```

```
Switch(dhcp-A-config)#netbios-name-server 10.16.1.209
Switch(dhcp-A-config)#netbios-node-type H-node
Switch(dhcp-A-config)#exit
Switch(Config)#ip dhcp excluded-address 10.16.1.200 10.16.1.210
Switch(Config)#ip dhcp pool B
Switch(dhcp-B-config)#network 10.16.2.0 24
Switch(dhcp-B-config)#lease 1
Switch(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201
Switch(dhcp-B-config)#dns-server 10.16.2.202
Switch(dhcp-B-config)#option 72 ip 10.16.2.209
Switch(dhcp-config)#exit
Switch(Config)#ip dhcp excluded-address 10.16.2.200 10.16.2.210
Switch(Config)#ip dhcp pool A1
Switch(dhcp-A1config)#host 10.16.1.210
Switch(dhcp-A1-config)#hardware-address 0003.2223.dcab
Switch(dhcp-A1-config)#    client-name management
Switch(dhcp-A1-config)#exit
```

Usage Guide When a DHCP/BootP client is connected to a VLAN1 port of the switch, the client can only get its address from 10.16.1.0/24 instead of 10.16.2.0/24. This is because the broadcast packet from the client will be requesting the IP address in the same segment of the VLAN interface after VLAN interface forwarding, and the VLAN interface IP address is 10.16.1.2/24, therefore the IP address assigned to the client will belong to 10.16.1.0/24.
If the DHCP/BootP client wants to have an address in 10.16.2.0/24, the gateway forwarding broadcast packets of the client must belong to 10.16.2.0/24. The connectivity between the client gateway and the switch must be ensured for the client to get an IP address from the 10.16.2.0/24 address pool.

18.3 DHCP Troubleshooting

18.3.1 Monitor and Debug Commands

18.3.1.1 clear ip dhcp binding

Command clear ip dhcp binding {*<address>* | all }
Function Deletes the specified IP address-hardware address binding record or all IP address-hardware address binding records.
Parameters ***<address>*** is the IP address that has a binding record in decimal format. **all** refers to all IP addresses that have a binding record.
Command mode Admin Mode
Relative Command show ip dhcp binding

18.3.1.2 clear ip dhcp conflict

Command clear ip dhcp conflict {*<address>* | all }

Function Deletes an address present in the address conflict log.

Parameters ***<address>*** is the IP address that has a conflict record; **all** stands for all addresses that have conflict records.

Command mode Admin Mode

Relative Command ip dhcp conflict logging，show ip dhcp conflict

18.3.1.3 clear ip dhcp server statistics

Command clear ip dhcp server statistics

Function Deletes the statistics for DHCP server, clears the DHCP server count.

Command mode Admin Mode

Relative Command show ip dhcp server statistics

18.3.1.4 show ip dhcp binding

Command show ip dhcp binding

Function Displays IP-MAC binding information.

Command mode Admin Mode

Displayed information	Explanation
IP address	IP address assigned to a DHCP client
Hardware address	MAC address of a DHCP client
Lease expiration	Valid time for the DHCP client to hold the IP address
Type	Type of assignment manual binding or dynamic assignment.

18.3.1.5 show ip dhcp conflict

Command show ip dhcp conflict

Function Displays log information for addresses that have a conflict record.

Command mode Admin Mode

Displayed information	Explanation
IP Address	Conflicting IP address
Detection method	Method in which the conflict is detected.
Detection Time	Time when the conflict is detected.

18.3.1.6 show ip dhcp server statistics

Command show ip dhcp server statistics

Function Displays statistics of all DHCP packets for a DHCP server.

Command mode Admin Mode

Displayed information	Explanation

Memory usage	using rate of EMS memory
Address pools	Number of DHCP address pools configured.
Database agents	Number of database agents.
Automatic bindings	Number of addresses assigned automatically
Manual bindings	Number of addresses bound manually
Conflict bindings	Number of conflicting addresses
Expiried bindings	Number of addresses whose leases are expired
Malformed message	Number of error messages.
Message Recieved	Statistics for DHCP packets received
BOOTREQUEST	Total packets received
DHCPDISCOVER	Number of DHCPDISCOVER packets
DHCPREQUEST	Number of DHCPREQUEST packets
DHCPDECLINE	Number of DHCPDECLINE packets
DHCPRELEASE	Number of DHCPRELEASE packets
DHCPINFORM	Number of DHCPINFORM packets
Message Send	Statistics for DHCP packets sent
BOOTREPLY	Total packets sent
DHCPOFFER	Number of DHCPOFFER packets
DHCPACK	Number of DHCPACK packets
DHCPNAK	Number of DHCPNAK packets
DHCPRELAY	Number of DHCPRELAY packets
DHCPFORWARD	Number of DHCPFORWARD packets

18.3.1.7 debug ip dhcp server

Command debug ip dhcp server { events|linkage|packets }

no debug ip dhcp server { events|linkage|packets }

Function Enables DHCP server debug information the "**no debug ip dhcp server { events|linkage|packets }"** command disables the debug information for DHCP server**.**

Default Debug information is disabled by default.

Command mode Admin Mode

18.3.1.8 debug ip dhcp client

Command debug ip dhcp cliet { events|packets }

no debug ip dhcp cliet { events|packets }

Function Enables DHCP server debug information the "**no debug ip dhcp cliet { events|packets }** "command command disables the debug information for DHCP server**.**

Default Debug information is disabled by default.

Command mode Admin Mode

18.3.2 DHCP Troubleshooting

If the DHCP clients cannot obtain IP addresses and other network parameters, the following procedures can be followed when DHCP client hardware and cables have been verified ok.

- Verify the DHCP server is running, start the related DHCP server if not running.
- If the DHCP clients and servers are not in the same physical network, verify the router responsible for DHCP packet forwarding has DHCP relay function. If DHCP relay is not available for the intermediate router, it is recommended to replace the router or upgrade its software to one that has a DHCP relay function.
- In such case, DHCP server should be examined for an address pool that is in the same segment of the switch VLAN, such a pool should be added if not present, and (This does not indicate SS2R24/48G4i switch switch cannot assign IP address for different segments, see solution 2 for details.)

In DHCP service, pools for dynamic IP allocation and manual binding are conflicting, i.e., if command "**network-address**" and "**host**" are run for a pool, only one of them will take effect; furthermore, in manual binding, only one IP-MAC binding can be configured in one pool. If multiple bindings are required, multiple manual pools can be created and IP-MAC bindings set for each pool. New configuration in the same pool overwrites the previous configuration.

Chapter 19 DHCP snooping Configuration

19.1 DHCP Snooping Introduction

DHCP Snooping can effectively block attacks from fake DHCP servers.

Defense against Fake DHCP Server once the switch intercepts the DHCP server reply packets from un-trusted ports(including DHCPOFFER, DHCPACK, and DHCPNAK), it will alarm the users and respond according to the situation(shutdown the port or send BlackHole)。

Defense against DHCP over load attacks To avoid too many DHCP messages attacking CPU, users should limit the speed of DHCP to receive packets on trusted and un-trusted ports.

Record the binding data of DHCP DHCP SNOOPING will record the binding data of DHCP SERVER while forwarding DHCP messages, it can also upload the binding data to the specified server to backup it. The binding data is mainly used to configure the dynamic users of dot1x userbased ports. Please refer to the chapter named “dot1x configuration” to find more about the usage of dot1x userbased mode.

Automatic Recovery A while after the switch shut down the port or sent blockhole , it should automatically recover the communication of the port or source MAC and send information to Log Server via syslog

LOGF Function When the switch discovers abnormal received packets or automatically recovers, it should send syslog information to Log Server

19.2 DHCP Snooping Configuration

19.2.1 DHCP Snooping Configuration Task Sequenc

1. Enable DHCP Snooping
2. Enable the binding function of DHCP Snooping
3. Configure helper server address
4. Configure trusted ports
5. Configure defense action
6. Set log record

1.Enable DHCP Snooping

Command	Explanation
Global configuration mode	

Ip dhcp snooping enable **no Ip dhcp snooping enable**	Enable or disable dhcp snooping function

2.Enable the binding function of DHCP Snooping

Command	Explanation
Global configuration mode	
Ip dhcp snooping binding enable **no Ip dhcp snooping binding enable**	Enable or disable the binding function of dhcp snooping

3.Set trusted ports

Command	Explanation
Port configuration mode	
Ip dhcp snooping trust **no Ip dhcp snooping trust**	Set or delete the dhcp snooping trust attributes of the port.

4. Configure defense action

Command	Explanation
Port configuration mode	
ip dhcp snooping action {shutdown|blackhole} [recovery <second>] **no ip dhcp snooping action**	Set or delete the automatic defense action of the port.

5.Set the helper server address

Command	Explanation
Global configuration mode	
Ip user helper-address <*svr_addr*> [port <*udp_port*>] source <*src_addr*> [secondary] **No ip user helper-address [secondary]**	Configure/delete HELPER SERVER address

6.Enable the debug switch

Command	Explanation
Admin Mode	
Debug ip dhcp snooping packet **Debug ip dhcp snooping event**	Please refer to the chapter on system debugging

7.Set log record

Command	Explanation
Admin Mode	
Login on **logging source {default | m_shell|sys_event|anti_attack} channel { console | logbuff | loghost | monitor } [level { critical | debugging | notifications | warnings } [state { on | off }]]**	Please refer to the chapter on system log

19.2.2 DHCP Snooping Typical Applications

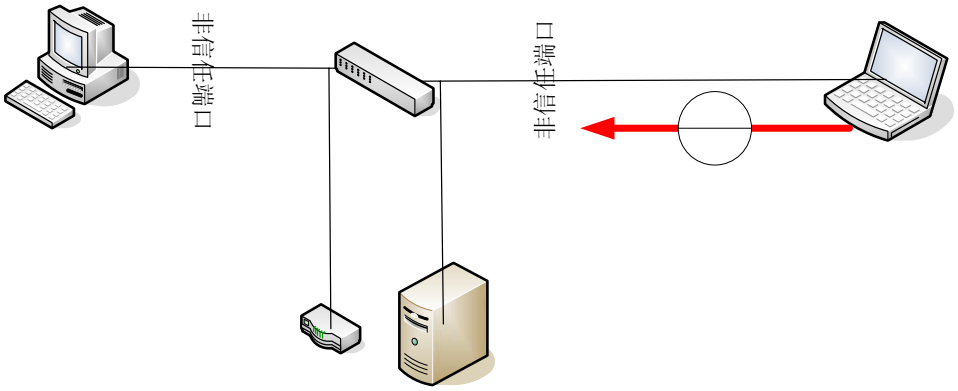


Fig18-1

As showed in the above picture, Mac-AA device is the normal user，connected to the un-trusted port 0/0/1 of the DCN switch. It acts as DHCP Client, and its IP is 1.1.1.5;DHCP Server and GateWay connect to the trusted ports 0/0/11 and 0/0/12 of the DCN switch; malicious user Mac-BB connects to the un-trusted port 0/0/10, trying to fake a DHCP Server(by sending DHCPACK). Configuring DHCP Snooping on the switch will effectively discover and block such network attacks.

The followings are the configuration sequence

```
switch#
switch#config
switch(Config)#ip dhcp snooping
switch(Config)#interface ethernet 0/0/11
switch(Config-Ethernet0/0/11)#ip dhcp snooping trust
switch(Config-Ethernet0/0/11)#exit
switch(Config)#interface ethernet 0/0/12
switch(Config-Ethernet0/0/12)#ip dhcp snooping trust
switch(Config-Ethernet0/0/12)#exit
switch(Config)#interface ethernet 0/0/1-10
switch(Config-Port-Range)#ip dhcp snooping action shutdown
```

switch(Config-Port-Range)#

19.3 DHCP Snooping Troubleshooting

19.3.1 Monitor and Debug Information

19.3.1.1 show ip dhcp snooping

Command show ip dhcp snooping [interface [ethernet] <interfaceName>]

Function Display the configuration information of the current dhcp snooping or display the defense action log of the specified port.

Parameters

<interfaceName> The name of the specified port

Command Mode Admin Mode

Default Setting None

Displayed information	Explanation
DHCP Snooping is enable	DHCP Snooping is globally enabled or disabled
interface	Name of the port
trust	Trust attributes of the port
action	Automatic defense action of the port
recovery	The recovery interval of the automatic defense action of the port
alarm num	The history log number of the automatic defense action of the port

Displayed information	Explanation
interface	Name of the port
trust attribute	Trust attributes of the port
action	Automatic defense action of the port
recovery interval	The recovery interval of the automatic defense action of the port
maxnum of alarm info	The max number of the automatic defense action that can be recorded of the port
Under the line	The history log of the automatic defense action of the port

19.3.1.2 logging source

Command **logging source {default | m_shell|sys_event|anti_attack} channel { console | logbuff | loghost | monitor } [level { critical | debugging | notifications | warnings } [state { on | off }]]**

Function The details about this command are covered in the chapter on system log; the data source of this command anti_attack records information about all kinds of denfense to network attacks, including the automatic defense action log of dhcp snooping.

Parameters Not covered

Command Mode Global configuration mode

Default Setting Not covered

19.3.1.3 show logging lastFailureInfo

Command show logging lastFailureInfo

Function This command is used to display the system abnormal information recorded in the flash. The defense action of DHCP Snooping is also recorded in the flash as system abnormal information, and can be checked via this command.

Command Mode Admin Mode

19.3.2 DHCP SnoopingTroubleshooting

If there are problems when using DHCP Snooping, please check the following possible reasons

- ✧ Check whether the global DHCP Snooping switch is enabled;
- ✧ If the port does not response to invalid DHCP Server packets, please check whether the port has been set as an un-trusted port of dhcp snooping.

19.3.2.1 debug ip dhcp snooping packet

Command debug ip dhcp snooping packet

no debug ip dhcp snooping packet

Function This command is used to enable the DHCP SNOOPING debug switch to debug the procedure of message processing.

Command Mode Admin Mode

19.3.2.2 debug ip dhcp snooping event

Command debug ip dhcp snooping event

no debug ip dhcp snooping event

Function This command is used to enable the DHCP SNOOPING debug switch to debug the state of DHCP SNOOPING tasks.

Command Mode Admin Mode

Chapter 20 Defense Against Segment Scanning

20.1 Defense Against Segment Scanning

20.1.1 Defense Against Segment Scanning Configuration Task Sequence

1. Enable the defense against segment scanning function
2. Configure trusted ports
3. Configure trusted source IP
4. Enable the log recording function
5. Enable the automatic recovery function
6. Set the automatic recovery interval
7. Set the limit of the message rate

1. Enable the defense against segment scanning function

Command	Explanation
Global configuration mode	
anti-netscan enable **no anti-netscan enable**	Enable/disable the defense against segment scanning function。

2. Configure trusted ports

Command	Explanation
Port configuration mode	
anti-netscan trust port **no anti-netscan trust port**	Set a port as a trusted port / cancel the setting

3. Configure trusted source IP

Command	Explanation
Global configuration mode	
anti-netscan trust ip ***<IPAddress> [<Mask>]*** **no anti-netscan trust ip** ***<IPAddress> [<Mask>]***	Add/delete trusted source IP.

4. Enable the log recording function

Command	Explanation
Global configuration mode	
anti-netscan log enable **no anti-netscan log enable**	Enable/disable the log recording function.

5. Enable the automatic recovery function

Command	Explanation
Global configuration mode	
anti-netscan recovery enable **no anti-netscan recovery enable**	Enable /disable the automatic recovery function

6. Set the automatic recovery interval

Command	Explanation
Global configuration mode	
anti-netscan recovery time <*seconds*> **no anti-netscan recovery time**	Set the automatic recovery interval; the “no anti-netscan recovery time ” will reset it to the default value.

7. Set the limit of the message rate

Command	Explanation
Global configuration mode	
anti-netscan limit-rate <*pps*> **no anti-netscan limit-rate**	Set the limit of the message rate, the ” no anti-netscan limit-rate” will reset it to the default value.

20.1.2 Monitor and Debug Command

20.1.2.1 show anti-netscan

Command show anti-netscan

Function To display the information of defense against segment scanning

Command Mode Admin Mode

Displayed Information	Explanation
Anti-netscan task interval	ANTI-NETSCAN task interval in second
Anti-netscan rate limit	Message rate limit, in pps
Shut port	The list of shut ports
Disabled IP	The disabled source IP list
Total	The total number of the disabled source IP.

Chapter 21 SNTP Configuration

The Network Time Protocol (NTP) is widely used for clock synchronization for global computers connected to the Internet. NTP can assess packet sending/receiving delay in the network, and estimate the computer's clock deviation independently, so as to achieve high accuracy in network computer clocking. In most positions, NTP can provide accuracy from 1 to 50ms according to the characteristics of the synchronization source and network route.

Simple Network Time Protocol (SNTP) is the simplified version of NTP, removing the complex algorithm of NTP. SNTP is used for hosts who do not require full NTP functions, it is a subset of NTP. It is common practice to synchronize the clocks of several hosts in local area network with other NTP hosts through the Internet, and use those hosts to provide time synchronization service for other clients in LAN. The figure below (Fig 3-1) depicts a NTP/SNTP application network topology, where SNTP mainly works between second level servers and various terminals since such scenarios do not require very high time accuracy, and the accuracy of SNTP (1 to 50 ms) is usually sufficient for those services.

SS2R24/48G4i switch switch implements SNTPv4 and supports SNTP client unicast as described in RFC2030; SNTP client multicast and unicast are not supported, nor is the SNTP server function.

21.1 Commands for SNTP

21.1.1 sntp server

Command sntp server <*server_address*> [version <*version_no*>]

no sntp server <*server_address*>

Function Configure the addresses and the version of the SNTP/NTP server; the "no" form of this command cancels the configured SNTP/NTP server addresses.

Parameter <*server_address*> is the IPv4 unicast address of the SNTP/NTP server, **<*version_no*>** is the version No. of the SNTP on current server,ranging between 1-4 and defaulted at 1.

Default No sntp/ntp configured by default.

Command Mode Global Mode

21.1.2 sntp polltime

Command sntp polltime <*interval*>

no sntp polltime

Function Sets the interval for SNTP clients to send requests to NTP/SNTP; the "**no sntp polltime**" command cancels the polltime sets and restores the default setting.Resume default value seconds

Parameters **< *interval*>** is the interval value from 16 to 16284

Default The default polltime is 64 seconds.

21.1.3 sntp timezone

Command sntp timezone *<name> {add | subtract} <time_difference>*

no sntp timezone

Function Set the time difference between the time zone in which the SNTP client resides and UTC. The "**no sntp timezone**" command cancels the time zone set and restores the default setting.

Parameter ***<name>*** is the time zone name, up to 16 characters are allowed; ***<add>*** means the time zone equals UTC time plus ***<time_difference>***; ***<subtract>*** means the time zone equals UTC time minus ***<time_difference>***; ***<time_difference>*** is the time difference, from 1 to 12.

Default The default time difference setting is "add 8".

Command mode Global Mode

21.1.4 show sntp

Command show sntp

Function To display the current configuration of SNTP client and the server state.

Parameters None

Command Mode Admin Mode.

Displayed Information	**Explanation**
server address	IP address of SNTP server;
version	The version of SNTP protocol;
last receive	The IP address of the last received SNTP server.

21.1.5 debug sntp

Command debug sntp {adjust | packet | select }

no debug sntp {adjust | packet | select}

Function Displays or disables SNTP debug information.

Parameters **adjust** stands for SNTP clock adjustment information; **packet** for SNTP packets, **select** for SNTP clock selection.

Command mode Admin Mode

21.2 Typical SNTP Configuration Examples

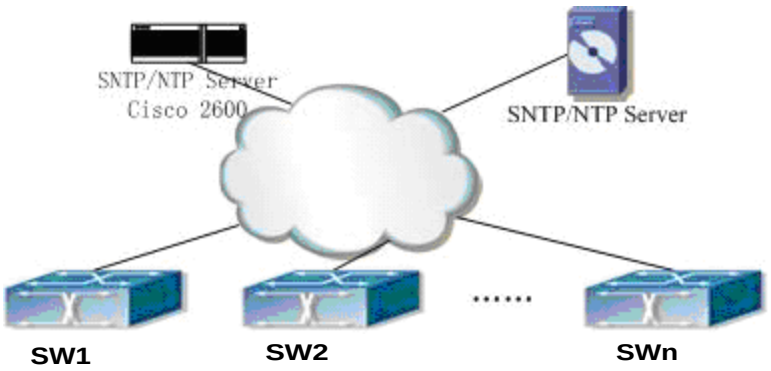


Fig 21-1 Typical SNTP Configuration

All SS2R24/48G4i switch switch in the autonomous zone are required to perform time synchronization, which is done through two redundant SNTP/NTP servers. For time to be synchronized, the network must be properly configured. There should be reachable route between any SS2R24/48G4i switch switch and the two SNTP/NTP servers.

Example　Assume the IP addresses of the SNTP/NTP servers are 10.1.1.1 and 20.1.1.1, respectively, and SNTP/NTP server function (such as NTP master) is enabled, then configurations for any SS2R24/48G4i switch switch should like the following

Switch #config
Switch (config)#sntp server 10.1.1.1
Switch (config)#sntp server 20.1.1.1
From now on, SNTP would perform time synchronization to the server according to the default setting (polltime 64s, version 1).

Chapter 22 QoS Configuration

22.1 Introduction to QoS

QoS (Quality of Service) is a set of capabilities that allow you to create differentiated services for network traffic, thereby providing better service for selected network traffic. QoS is a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate extra bandwidth but provides more effective bandwidth management according to the application requirement and network management policy.

22.1.1 QoS Terms

QoS Class of Service, the classification information carried by Layer 2 802.1Q frames, taking 3 bits of the Tag field in frame header, is called user priority level in the range of 0 to 7.

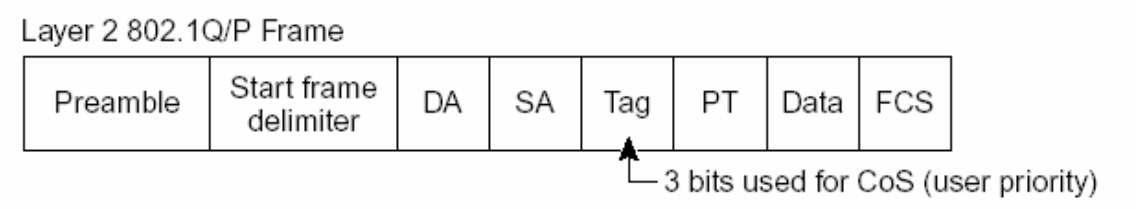


Fig 22-1 CoS priority

ToS Type of Service, a one-byte field carried in Layer 3 IPv4 packet header to symbolize the service type of IP packets. Among ToS field can be IP Precedence value or DSCP value.

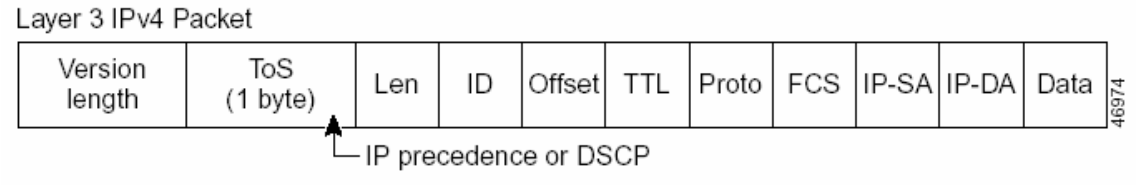


Fig 22-2 ToS priority

IP Precedence IP priority.Classification information carried in Layer 3 IP packet header, occupying 3 bits, in the range of 0 to 7.

DSCP Differentiated Services Code Point, classification information carried in Layer 3 IP packet header, occupying 6 bits, in the range of 0 to 63, and is downward compatible with IP Precedence.

Classification The entry action of QoS, classifying packet traffic according to the classification information carried in the packet and ACLs.

Policing Ingress action of QoS that lays down the policing policy and manages the classified packets.

Remark Ingress action of QoS, perform allowing, degrading or discarding operations to packets

according to the policing policies.

Queuing Egress QoS action. Put the packets to appropriate egress queues according to the packet CoS value.

Scheduling QoS egress action. Configure the weight for eight egress queues WRR (Weighted Round Robin).

In Profile Traffic within the QoS policing policy range (bandwidth or burst value) is called “In Profile".

Out of Profile Traffic out the QoS policing policy range (bandwidth or burst value) is called “Out of Profile".

22.1.2 QoS Implementation

To implement switch software QoS, a general, mature reference model should be given. QoS can not create new bandwidth, but can maximize the adjustment and configuration for the current bandwidth resource. Fully implemented QoS can achieve complete management over the network traffic. The following is as accurate as possible a description of QoS.

The data transfer specifications of IP cover only addresses and services of source and destination, and ensure correct packet transmission using OSI layer 4 or above protocols such as TCP. However, rather than provide a mechanism for providing and protecting packet transmission bandwidth, IP provide bandwidth service by the best effort. This is acceptable for services like Mail and FTP, but for increasing multimedia business data and e-business data transmission, this best effort method cannot satisfy the bandwidth and low-lag requirement.

Based on differentiated service, QoS specifies a priority for each packet at the ingress. The classification information is carried in Layer 3 IP packet header or Layer 2 802.1Q frame header. QoS provides same service to packets of the same priority, while offers different operations for packets of different priority. QoS-enabled switch or router can provide different bandwidth according to the packet classification information, and can remark on the classification information according to the policing policies configured, and may discard some low priority packets in case of bandwidth shortage.

If devices of each hop in a network support differentiated service, an end-to-end QoS solution can be created. QoS configuration is flexible, the complexity or simplicity depends on the network topology and devices and analysis to incoming/outgoing traffic.

22.1.3 Basic QoS Model

Classification Classify traffic according to packet classification information and generate internal DSCP value based on the classification information. For different packet types and switch configurations, classification is performed differently; the flowchart below explains this in detail

Policing and remark Each packet in classified ingress traffic is assigned an internal DSCP value and can be policed and remarked.

Policing can be performed based on DSCP value to configure different policies that allocate bandwidth to classified traffic. If the traffic exceeds the bandwidth set in the policy (out of profile), the out of profile traffic can be allowed, discarded or remarked. Remarking uses a new DSCP value of lower priority to

replace the original higher level DSCP value in the packet; this is also called “marking down”. The following flowchart describes the operations during policing and remarking

Queuing and scheduling Packets at the egress will re-map the internal DSCP value to CoS value, the queuing operation assigns packets to appropriate queues of priority according to the CoS value; while the scheduling operation performs packet forwarding according to the prioritized queue weight. The following flowchart describes the operations during queuing and scheduling.

22.2 QoS Configuration

22.2.1 QoS Configuration Task List

1. Enable QoS
   QoS can be enabled or disabled in Global Mode. QoS must be enabled first in Global Mode to configure the other QoS commands.
2. Configure class map.

Set up a classification rule according to ACL, VLAN ID, IP Precedence or DSCP to classify the data stream. Different classes of data streams will be processed with different policies.

3. Configure a policy map.
   After data steam classification, a policy map can be created to associate with the class map created earlier and enter class mode. Then different policies (such as bandwidth limit, priority degrading, assigning new DSCP value) can be applied to different data streams. You can also define a policy set that can be use in a policy map by several classes.
4. Apply QoS to the ports
   Configure the trust mode for ports or bind policies to ports. A policy will only take effect on a port when it is bound to that port.
5. Configure queue out method and weight
   Configure queue out to PQ or WRR, set the proportion of the 8 egress queues bandwidth and mapping from internal priority to egress queue.
6. Configure QoS mapping
   Configure the mapping from CoS to DSCP, DSCP to CoS, DSCP to DSCP mutation, IP precedence to DSCP, and policed DSCP.

1. Enable QoS

Command	**Explanation**
Global Mode	
mls qos **no mls qos**	Enable/disable QoS function.

2. Configure class map.

Command	**Explanation**
Global Mode	
class-map <*class-map-name*>	Create a class map and enter class

no class-map <*class-map-name*>	map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map.
match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*> | ip precedence <*ip-precedence-list*> | vlan <*vlan-list*>|*cos* <*cos-list*>} **no match {access-group | ip dscp | ip precedence | vlan |cos}**	Set matching criterion (classify data stream by ACL, DSCP, VLAN or priority, etc) for the class map; the "**no match {access-group | ip dscp | ip precedence | vlan |cos}**" command deletes specified matching criterion.

3. Configure a policy map.

Command	**Explanation**
Global Mode	
policy-map <*policy-map-name*> **no policy-map <*policy-map-name*>**	Create a policy map and enter policy map mode; the "**no policy-map <*policy-map-name*>**" command deletes the specified policy map.
class <*class-map-name*> **no class <*class-map-name*>**	After a policy map is created, it can be associated to a class. Different policy or new DSCP value can be applied to different data streams in class mode; the "**no class <*class-map-name*>**" command deletes the specified class.
set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>|*cos* <*new-cos*>} **no set {ip dscp | ip precedence |*cos*}**	Assign a new DSCP and IP precedence value for the classified traffic; the "**no set {ip dscp | ip precedence |*cos*}**" command cancels the newly assigned value.
police <*rate-bps*> <*burst-byte*> [exceed-action {drop | policed-dscp-transmit}] **no police <*rate-bps*> <*burst-byte*> [exceed-action {drop | policed-dscp-transmit}]**	Configure a policy to classify traffic, data stream exceeding the limit will be dropped or degraded; the "**no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]**" command deletes the specified policy.
mls qos aggregate-policer <*aggregate-policer-name*> <*rate-bps*> <*burst-byte*> exceed-action {drop |policed-dscp-transmit} **no mls qos aggregate-policer <*aggregate-policer-name*>**	Define a policy set, perform different actions to out-of-profile data streams, such as discard or degrade. This policy can be used in one policy map by several classes; the "**no mls qos aggregate-policer <*aggregate-policer-name*>**" command deletes the specified policy set.

police aggregate *<aggregate-policer-name>* **no police aggregate *<aggregate-policer-name>***	Apply a policy set to classified traffic; the "**no police aggregate *<aggregate-policer-name>***" command deletes the specified policy set.

4. Apply QoS to ports

Command	Explanation
Interface Mode	
mls qos trust [cos | dscp | port priority *<priority>*] **no mls qos trust**	Configure port trust; the "**no mls qos trust**" command disables the current trust status of the port.
mls qos cos {*<default-cos>* } **no mls qos cos**	Configure the default CoS value of the port; the "**no mls qos cos**" command restores the default setting.
service-policy {input *<policy-map-name>* | output *<policy-map-name>*} **no service-policy {input *<policy-map-name>* | output *<policy-map-name>*}**	Apply a policy map to the specified port; the "**no service-policy {input *<policy-map-name>* | output *<policy-map-name>*}**" command deletes the specified policy map applied to the port. Egress policy map is not supported yet.
mls qos dscp-mutation **no mls qos dscp-mutation**	Apply DSCP mutation mapping to the port; the "**no mls qos dscp-mutation** command restores the DSCP mutation mapping default.

5. Configure queue out method and weight

Command	Explanation
Interface Mode	
wrr-queue bandwidth *<weight1 weight2 weight3 weight4>* **no wrr-queue bandwidth**	Set the WRR weight for specified egress queue; the "**no wrr-queue bandwidth**" command restores the default setting.
priority-queue out **no priority-queue out**	Configure queue out method to pq method; the "**no priority-queue out**" command restores the default WRR queue out method.
wrr-queue cos-map *<queue-id> <cos1 ...*	Set CoS value mapping to specified

cos8> **no wrr-queue cos-map [<*queue-id*>]**	egress queue; the "**no wrr-queue cos-map[<*queue-id*>]**" command restores the default setting.

6. Configure QoS mapping

Command	Explanation
Global Mode	
mls qos map {cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*in-dscp*> to <*out-dscp*> | policed-dscp <*dscp-list*> to <*mark-down-dscp*>} **no mls qos map {cos-dscp | dscp-cos | dscp-mutation | policed-dscp}**	Set CoS to DSCP mapping, DSCP to CoS mapping, DSCP to DSCP mutation mapping, IP precedence to DSCP and policed DSCP mapping; the "**no**"command restores the default mapping.

22.3 QoS Example

Scenario 1

Enable QoS function, change the queue out weight of port ethernet 0/0/1to 1 2 4 8, and set the port in trust QoS mode without changing DSCP value, and set the default QoS value of the port to 5.

The configuration steps are listed below

Switch#config

Switch(config)#mls qos
Switch(config)#wrr-queue bandwidth 1 2 4 8
Switch(config)#interface ethernet 0/0/1
Switch(config-Ethernet0/0/1)#mls qos trust cos
Switch(config-Ethernet0/0/1)#mls qos cos 5
Configuration result

When QoS enabled in Global Mode, the egress queue bandwidth proportion of port ethernet 0/0/1 is 1 2 4 8. When packets have CoS value coming in through port ethernet 0/0/1, it will be map to the queue out according to the CoS value, CoS value 0 to 7 correspond to queue out 1, 1, 2, 2, 3,3,4, 4, respectively. If the incoming packet has no CoS value, it is default to 5 and will be put in queue 6. All passing packets would not have their DSCP values changed.

Scenario 2

In port ethernet 1/2, set the bandwidth for packets from segment 192.168.1.0 to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting will be dropped.
The configuration steps are listed below

Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#mls qos

```
Switch(config)#class-map c1
Switch(config-ClassMap)#match access-group 1
Switch(config-ClassMap)# exit
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config--Policy-Class)#police 10000000 4000 exceed-action drop
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit
Switch(config)#interface ethernet 0/0/2
Switch(Config-Ethernet0/0/2)#service-policy input p1
```

Configuration result

An ACL name 1 is set to matching segment 192.168.1.0. Enable QoS globally, create a class map named c1, matching ACL1 in class map; create another policy map named p1 and refer to c1 in p1, set appropriate policies to limit bandwidth and burst value. Apply this policy map on port ethernet 0/0/2. After the above settings done, bandwidth for packets from segment 192.168.1.0 through port ethernet 0/0/2 is set to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting in that segment will be dropped.

Scenario 3

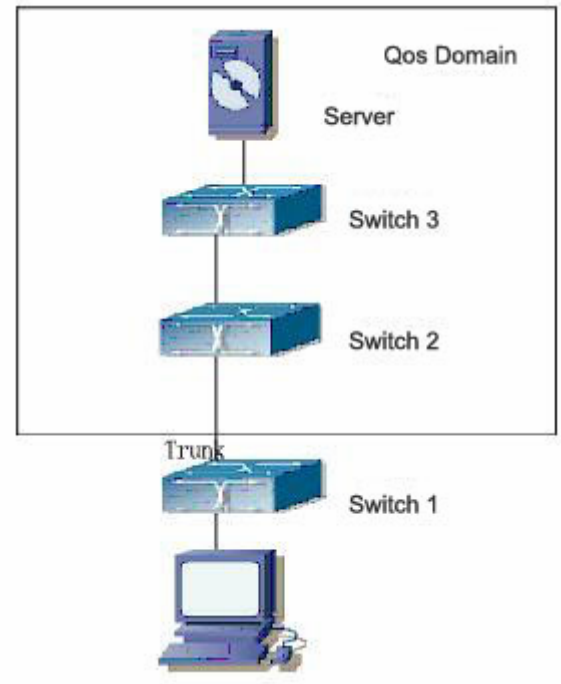


Fig 22-3 Typical QoS topology

As shown in the figure, inside the block is a QoS domain, SwitchA classifies different traffics and

assigns different IP precedences. For example, set IP precedence for packets from segment 192.168.1.0 to 5 on port ethernet 1/1. The port connecting to switch2 is a trunk port. In SwitchB, set port ethernet 1/1 that connecting to swtich1 to trust IP precedence. Thus inside the QoS domain, packets of different priorities will go to different queues and get different bandwidth.

The configuration steps are listed below

QoS configuration in Switch1

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(config-ClassMap)#match access-group 1
Switch(config-ClassMap)# exit
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config--Policy-Class)#set ip precedence 5
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit
Switch(config)#interface ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#service-policy input p1
```

QoS configuration in Switch2

```
Switch#config
Switch(config)#mls qos
Switch(config)#interface ethernet 0/0/1
Switch(config-Ethernet0/0/1)#mls qos trust cos
```

22.4 QoS Troubleshooting

22.4.1 QoS Monitor And Debug Command

22.4.1.1 show mls-qos

Function Displays global configuration information for QoS.
Parameters N/A.
Default N/A
Command mode Admin Mode

Displayed information	Explanation
Qos is enabled	QoS is enabled.

22.4.1.2 show mls qos aggregate-policer

Command **show mls qos aggregate-policer [<*aggregate-policer-name*>]**
Function Displays policy set configuration information for QoS.

Parameters ***<aggregate-policer-name>*** is the policy set name.
Default N/A.
Command mode Admin Mode

Displayed information	Explanation
aggregate-policer policer1 80000 80 exceed-action drop	Configuration for this policy set.
Not used by any policy map	Time that the policy set is being referred to

22.4.1.3 show mls qos interface

Command **show mls qos interface [*<interface-id>*] [buffers | policers | queueing | statistics]**
Function Displays QoS configuration information on a port.
Parameters ***<interface-id>*** is the port ID; **buffers** is the queue buffer setting on the port; **policers** is the policy setting on the port; **queuing** is the queue setting for the port; **statistics** is the number of packets allowed to pass for in-profile and out-of-profile traffic according to the policy bound to the port.
Default N/A.
Command mode Admin Mode

Displayed information	Explanation
Ethernet1/2	Port name
default cos 0	Default CoS value of the port.
DSCP Mutation Map Default DSCP Mutation Map	Port DSCP map name
Attached policy-map for Ingress p1	Policy name bound to port.

Displayed information	Explanation
Ethernet0/0/2	Port name
buffer size of 4 queue 256 256 256 256	Available buffer number for all 4 queues out on the port, this is a fixed setting that cannot be changed.

Displayed information	Explanation
Cos-queue map Cos 0 1 2 3 4 5 6 7 Queue 1 1 2 2 3 3 4 4	CoS value to queue mapping.
Queue and weight type q1 q2 q3 q4 QType 1 2 4 8 WFQ	Queue to weight mapping.

Displayed information	Explanation
Ethernet1/2	Port name
Attached policy-map for Ingress p1	Policy map bound to the port.

Displayed information	Explanation
Ethernet1/2	Port name
ClassMap	Name of the Class map
Classified	Total data packets match this class map.
In-profile	Total in-profile data packets match this class map.
out-profile	Total out-profile data packets match this class map.

22.4.1.4 show mls qos maps

Command show mls qos maps [cos-dscp | dscp-cos | dscp-mutation | policed-dscp]
Function Displays mapping configuration information for QoS.
Parameter **cos-dscp** CoS for CoS-DSCP; **dscp-cos** DSCP for DSCP-CoS, **dscp-mutation** for DSCP-DSCP mutation, **policed-dscp** is DSCP mark down mapping
Default N/A.
Command mode Admin Mode

22.4.1.5 show class-map

Command show class-map [<*class-map-name*>]
Function Display class map of QoS.
Parameter **< *class-map-name*> is the class map name.**
Default N/A.
Command mode Admin Mode
Usage Guide
Example

Switch # show class-map
Class map name c1
Match acl name 1

Displayed information	Explanation
Class map name c1	Name of the Class map
Match acl name 1	Classifying rule for the class map.

22.4.1.6 show policy-map

Command **show policy-map [<*policy-map-name*>]**
Function Display policy map of QoS.
Parameter **< *policy-map-name*> is the policy map name.**
Default N/A.
Command mode Admin Mode

Displayed information	Explanation
Policy Map p1	name of policy map
Class map name c1	Name of the class map referred to
police 16000000 8000 exceed-action drop	Policy implemented

22.4.2 Qos Troubleshooting

- QoS is disabled on switch ports by default, 4 sending queues are set by default, queue1 forwards normal packages, other queues are used for some important control packets (such as BPDU). Choose an array according to the Cos value when QoS is shut down
- When QoS is enabled in Global Mode,. QoS is enabled on all ports with 4 traffic queues. The default CoS value of the port is 0; port is in not Trusted state by default; the default queue weight values are 1, 2, 4, 8 in order, all QoS Map is using the default value.
- CoS value 7 maps to queue 4 that has the highest priority and usually reserved for certain protocol packets. It is not recommended for the user to change the mapping between CoS 7 to Queue 4, or set the default port CoS value to 7.
- Policy map can only be bound to ingress direction, egress is not supported yet.
- If the policy is too complex to be configured due to hardware resource limit, error massages will be provided.

Chapter 23 Layer 3 Configuration

SS2R24/48G4i switch switch only supports layer 2 forwarding function. But, we can configure a layer3 control port. On the interface of this port we can configure IP addresses used in communication of various IP-based control protocols.

23.1 Layer3 Interface

23.1.1 Introduction to Layer3 Interface

Layer3 interface can be created on SS2R24/48G4i switch. Layer3 interface is not physical interface but a virtual interface. Layer3 interface is built on VLAN. Layer3 interface can contain one or more layer2 interface of the same VLAN, or no layer2 interfaces. At least one of Layer2 interfaces contained in Layer3 interface should be in UP state for Layer3 interface in the UP state, otherwise, Layer3 interface will be in the DOWN state. All layer3 interface in the switch use the same MAC address, this address is selected from the reserved MAC address on creating Layer3 interface. Layer3 interface is the base for layer3 protocols. The switch can use the IP address set in layer3 interface to communicate with the other devices via IP. The switch can forward IP packets between different Layer3 interfaces.

23.1.2 Layer3 interface configuration

23.1.2.1 Layer3 Interface Configuration Task Sequence

1. Create Layer3 Interface
2. Set the default gateway address of the switch

1.Create Layer3 Interface
2. Set the default gateway address of the switch

Command	**Explanation**
Global Mode	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	Create a VLAN interface (VLAN interface is a Layer3 interface); the “**no interface vlan <*vlan-id*>**” command deletes the VLAN interface (Layer3 interface) created in the switch.
Global Mode	
ip route 0.0.0.0 0.0.0.0 <gateway> **no ip route 0.0.0.0 0.0.0.0 <gateway>**	Set the default gateway address of the switch; prefixing this command with “no”

	will delete the default gateway address.

23.2 ARP

23.2.1 Introduction to ARP

ARP (Address Resolution Protocol) is mainly used in IP address to Ethernet MAC address resolution. SS2R24/48G4i switch supports static configuration.

23.2.1.1 ARP Configuration Task Sequence

1. Configure static ARP

Command	Explanation
arp <*ip_address*> <*mac_address*> **no arp <*ip_address*>**	Configure a static ARP entry; the "**no arp <*ip_address*>"** command deletes a static ARP entry.

23.2.2 ARP Forwarding Troubleshooting

23.2.2.1 Monitor and Debug Commands

23.2.2.1.1show arp

Comman show arp [<*ip-addr*>][<*vlan-id*>][<*hw-addr*>][type {static|dynamic}][count]

Function Display the ARP table.

Parameter **<*ip-addr*>** is a specified IP address; **<*vlan-id*>** stands for the entry for the identifier of specified VLAN; **<*hw-addr*>** for entry of specified MAC address; "**static**" for static ARP entry; "**dynamic**" for dynamic ARP entry; "**count**" displays number of ARP entries.

Command mode Admin Mode

Command	Explanation
Addrss	IP address of Arp entries 2.2.2.66
Hardware Address	MAC address of Arp entries 00-10-00-00-00-C5
Interface	Layer3 interface corresponding to the ARP

	entry.
Port	Physical (Layer2) interface corresponding to the ARP entry.
Flag	Describes whether ARP entry is dynamic or static.

23.2.2.1.2debug arp

Command **debug arp**

no debug arp

Function Enable the ARP debug function the "**no debug arp**" command disables this debug function.

Default ARP debug is disabled by default.

Command mode Admin Mode

23.2.2.2 ARP Troubleshooting Help

If ping from the switch to directly connected network devices fails, the following can be used to check the possible cause and solution.

- Check whether the corresponding ARP has been learned by the switch.
- If ARP is not learned, then enabled ARP debug information and view sending/receiving condition of ARP packets.